

(12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関  
国際事務局(43)国際公開日  
2004年2月5日 (05.02.2004)

PCT

(10)国際公開番号  
WO 2004/012085 A1

(51)国際特許分類<sup>7</sup>: G06F 12/14, G11B 20/10, G06F 3/06, H04N 5/91

(21)国際出願番号: PCT/JP2003/009414

(22)国際出願日: 2003年7月24日 (24.07.2003)

(25)国際出願の言語: 日本語

(26)国際公開の言語: 日本語

(30)優先権データ: 特願2002-216750 2002年7月25日 (25.07.2002) JP

(71)出願人(米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP];

〒570-8677 大阪府 守口市 京阪本通2丁目5番5号 Osaka (JP). パイオニア株式会社 (PIONEER CORPORATION) [JP/JP]; 〒153-8654 東京都 目黒区 目黒1丁目4番1号 Tokyo (JP). 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都 千代田区 神田駿河台四丁目6番地 Tokyo (JP). フェニックステクノロジーズ株式会社 (PHOENIX TECHNOLOGIES, K.K.) [JP/JP]; 〒100-0005 東京都 千代田区 丸の内1丁目3番地1 東京銀行協会ビル14階 Tokyo (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区上小田中4丁目1番1号 Kanagawa (JP).

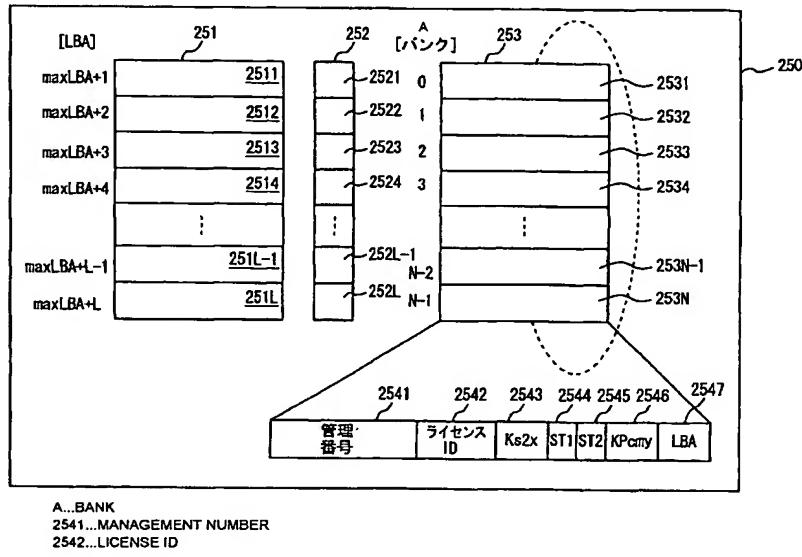
(72)発明者; および

(75)発明者/出願人(米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府 守口市 京阪本通2丁目5番5号 三洋電機株式会社内

(統葉有)

(54) Title: Data storage device capable of storing multiple SETS of history information on input/output processing of security data without duplication

(54)発明の名称: 機密データの入出力処理に関する履歴情報を重複することなく複数格納できるデータ記憶装置



(57) Abstract: A data storage device comprises a secure data storage unit (250) including a log memory (253). The log memory (253), composed of multiple banks (2531 to 253N), stores history information in the multiple banks (2531 to 253N) in a ring. Each of the multiple banks (2531 to 253N) is specified by an address (0 to N-1). The history information stored in each of the banks (2531 to 253N) comprises a management number area (2541), a license ID (LID) area (2542), a Ks2x area (2543), an ST1 area (2544), an ST2 area (2545), a KPcmy area (2546), and an LBA area (2547).

(57)要約: データ記憶装置は、ログメモリ(253)を含むセキュアデータ記憶部(250)を備える。ログメモリ(253)は、複数のバンク(2531～253N)から成り、複数のバンク(2531～253N)にリング状に履歴情報を格納する。複数のバンク(2531～253N)の各々は、

(統葉有)

WO 2004/012085 A1



Osaka (JP). 多田 謙一郎 (TADA, Kenichiro) [JP/JP]; 〒359-8522 埼玉県 所沢市 花園 4 丁目 2 6 1 O 番地 パイオニア株式会社 所沢工場内 Saitama (JP). 平井 達哉 (HIRAI, Tatsuya) [JP/JP]; 〒215-0013 神奈川県 川崎市 麻生区 王禅寺 1 0 9 9 番地 株式会社 日立製作所 システム開発研究所内 Kanagawa (JP). 津留 雅文 (TSURU, Masafumi) [JP/JP]; 〒100-0005 東京都 千代田区 丸の内 1 丁目 3 番地 1 東京銀行協会ビル 14 階 フェニックステクノロジーズ 株式会社内 Tokyo (JP). 長谷部 高行 (HASEBE, Takayuki) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区 上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府 大阪市 北区 南森町 2 丁目 1 番 2 9 号 三井住友銀行 南森町ビル 深見特許事務所 Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,

ID, IL, IN, IS, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイドラインスノート」を参照。

## 明細書

機密データの入出力処理に関する履歴情報を  
重複することなく複数格納できるデータ記憶装置

5

## 技術分野

この発明は、機密データの読み出し処理および書き込み処理を安全に提供するデータ記憶装置に関し、特に、著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶し、マルチアクセスが可能なデータ記憶装置においてコピーされた情報に対する著作権保護を可能とするデータ記憶装置に関するものである。

## 背景技術

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとつても、かえって不利益となる。

しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセンスを識別するためのライセンス ID、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築し、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。最終的に、携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

また、メモリカードは、他のメモリカードとの間でライセンスの移動または複

5 製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

10 さらに、送受信中の不慮の中断によってライセンスが消失した場合に、その処理を再開でき、かつ、ライセンスの重複送信を防ぐためにライセンスの入出力に関する直近の履歴情報を記録し、必要に応じて出力する機能をメモリカードは備えている。送信元である配信サーバあるいはメモリカードは、送信先のメモリカードから履歴情報を取得して、この履歴情報に従ってライセンスの送受信の再開を判断する。履歴情報は、ライセンス ID と送受信を示すステータス情報を含んでいる。

15 このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。また、著作権者の権利を保護することができる。

20 しかし、従来のメモリカードにおいては、直近の履歴情報を保持するのみで、中断後、他のライセンスに対する送受信を行った場合に先の中断に対する履歴情報が消えてしまう。このような場合、複数の履歴情報を格納することにより、ユーザの利便性を改善することが可能である。

また、記憶素子に対するアクセスの高速化や、記憶素子の大容量化に伴い、複数のライセンスの送受信を並行して行なう要求が発生することが、今後、予想される。その場合、少なくとも並行して行われる処理に関する履歴情報を格納できるようにする必要性が生ずる。

25 このように、複数の履歴情報を格納できるようにする場合に、ライセンスの受信後に、該ライセンスを他のメモリカードに対して移したとすると、同一のライセンス ID に対して異なったステータスを持つ履歴情報が格納されるという問題が生じる。

## 発明の開示

それゆえに、この発明の目的は、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための履歴情報を重複することなく複数格納できるデータ記憶装置を提供することである。

5 なお、この発明は、コンテンツデータに対するライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大され得る。

したがって、この発明によれば、データ記憶装置は、一定の手順に従って機密データの入出力を行ない、機密データを記憶し、かつ、一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を隨時更新するデータ記憶装置であって、  
10 外部とデータの入出力を行なうインターフェースと、複数の機密データを格納するデータ記憶部と、機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、機密データの入出力を制御する制御部とを備え、ログ記憶部は、それぞれ 1 つの履歴情報を格納する 2 つ以上の領域を循環的に利用するリングバッファとして設けられており、ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、制御部は、機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に受取った識別情報を含む機密データの入出力処理に対する履歴情報を新たに格納する。  
15  
20

好ましくは、履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、制御部は、入出力の対象となる機密データの識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、最新領域に格納されている履歴情報の一部または全てをインターフェースを介して出力する。  
25

好ましくは、履歴情報の出力を伴う前記機密データの入力処理において、制御部は、入出力の対象となる機密データの識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識

別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの入力処理に対する新たな履歴情報として格納し、特定された最古領域に格納された履歴情報の一部または全てをインターフェースを  
5 介して出力する。

好ましくは、他の装置によって一定の手順の進行によって記録されたもう1つの履歴情報の入力を伴う機密データの再出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報とをインターフェースを  
10 介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

好ましくは、他の装置によって一定の手順の進行に従って記録されたもう1つの履歴情報の入力を伴う機密データの出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報をインターフェースを  
15 介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの出力処理に対する新たな履歴情報として格納し、特定した最古領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

20 好ましくは、最古領域を特定した後、制御部は、入出力処理における一定の手順が終了あるいは中止されるまでの間、特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する。

好ましくは、複数の履歴情報の各々は、ログ記憶部へ記憶された順序を識別するための管理番号をさらに含み、管理番号は、ログ記憶部に連続して配置された  
25 2つの領域に格納された2つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される最古領域を検出する。

好ましくは、ログ記憶部は、N (Nは2以上の自然数) 個の領域を循環的に利用するリングバッファからなり、管理番号は、M (Mは、N < Mを満たす自然数) の剩余系からなる。

好ましくは、制御部は、ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号を取得し、その取得した2つの管理番号の差に基づいて、2つの当該管理番号を含む2つの履歴情報が連続して格納されたか否かを判定し、2つの履歴情報が不連続に格納された履歴情報である  
5 とき、連続する2つの領域のうち、後続領域を最古領域として検出する。

したがって、この発明によれば、機密データを保護し、かつ、機密データの入出力処理に関する複数の履歴情報を重複することなく格納し、出力あるいは参照できる。

## 10 図面の簡単な説明

図1は、データ配信システムを概念的に説明する概略図である。

図2は、図1に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

図3は、図1に示すデータ配信システムにおいて使用される暗号通信に用いられる鍵、情報等の特性を示す図である。  
15

図4は、図1に示すライセンス提供装置の構成を示す概略ブロック図である。

図5は、図1に示す端末装置の構成を示す概略ブロック図である。

図6は、図1に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

図7は、図6に示すハードディスクにおけるセキュアデータ記憶部の構成を示す図である。  
20

図8は、図6に示すハードディスクにおけるノーマルデータ記憶部の構成を示す図である。

図9は、図1に示すデータ配信システムにおける配信処理を説明するための実施の形態1における第1のフローチャートである。  
25

図10は、図1に示すデータ配信システムにおける配信処理を説明するための実施の形態1における第2のフローチャートである。

図11は、図9に示すステップS20の詳細な動作を説明するためのフローチャートである。

図12は、図11に示すステップS20aの詳細な動作を説明するためのフローチャートである。

図13は、図1に示すデータ配信システムにおける配信処理中の再書き込み処理を説明するための実施の形態1における第1のフローチャートである。

5 図14は、図1に示すデータ配信システムにおける配信処理中の再書き込み処理を説明するための実施の形態1における第2のフローチャートである。

図15は、図1に示すデータ配信システムにおける配信処理中の再書き込み処理を説明するための実施の形態1における第3のフローチャートである。

10 図16は、図13に示すステップS112aの詳細な動作を説明するためのフローチャートである。

図17は、複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

図18は、図17に示すシステムにおける複製または移動処理を説明するための実施の形態1における第1のフローチャートである。

15 図19は、図17に示すシステムにおける複製または移動処理を説明するための実施の形態1における第2のフローチャートである。

図20は、図18に示すステップS218の詳細な動作を説明するためのフローチャートである。

20 図21は、図17に示すシステムにおける複製または移動処理中の再書き込み処理を説明するための実施の形態1における第1のフローチャートである。

図22は、図17に示すシステムにおける複製または移動処理中の再書き込み処理を説明するための実施の形態1における第2のフローチャートである。

図23は、図17に示すシステムにおける複製または移動処理中の再書き込み処理を説明するための実施の形態1における第3のフローチャートである。

25 図24は、図5に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

図25は、図1に示すデータ配信システムにおける配信処理を説明するための実施の形態5における第1のフローチャートである。

図26は、図1に示すデータ配信システムにおける配信処理を説明するための

実施の形態 5 における第 2 のフローチャートである。

図 27 は、図 25 に示すステップ S 16 a の詳細な動作を説明するためのフローチャートである。

図 28 は、図 17 に示すシステムにおける複製または移動処理を説明するため 5 の実施の形態 5 における第 1 のフローチャートである。

図 29 は、図 17 に示すシステムにおける複製または移動処理を説明するための実施の形態 5 における第 2 のフローチャートである。

図 30 は、図 28 に示すステップ S 208 の詳細な動作を説明するためのフローチャートである。

10

### 発明を実施するための最良の形態

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

#### [実施の形態 1]

15 図 1 は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

なお、以下では、デジタル放送網により配信された映像データを端末装置 10 により受信して端末装置 10 に装着されたデータ記憶装置である HD (ハードディスクドライブ) 20 に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク 30 に端末装置 10 と接続されるライセンス提供装置 40 からネットワーク 30 を介してから受信して HD 20 に格納し、暗号化された映像データを端末装置 10 に内蔵された専用の再生回路 (図示せず) にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモ

リカードなどにおいても適用することが可能である。

図1を参照して、端末装置10は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ11を介して受信し、HD20に記憶する。暗号化されたコンテンツデータ（以下、暗号化コンテンツデータとも呼ぶ）を復号するためのコンテンツ鍵を含むライセンスを管理し、かつ、配信するライセンス提供装置40は、ライセンスの配信を求めてアクセスしてきた端末装置10に装着されたHD20が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、HD20が正当なデータ記憶装置であった場合のみ、端末装置10に対してHD20においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置10は、ネットワーク30に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着されたHD20へ送信する。

図1においては、たとえば、HD20は、端末装置10に着脱可能な構成となっている。端末装置10に装着されたHD20は、端末装置10により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえでHD20内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置10に与える。

そして、端末装置10のユーザは、端末装置10においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

このような構成とすることで、端末装置10のユーザは、ライセンス管理機能を備えた正規の認証データを有するHD20を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、ライセンスを管理するライセンス提供装置40であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置40とは別の配信サーバであってもよい。また、他の

ユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

5 したがって、本発明の実施の形態においては、HD 20、端末装置10およびライセンス提供装置40のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したときに、ライセンスが重複して存在するないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

図2は、図1に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

15 データDcは、コンテンツデータであって、ここでは映像データである。データDcは、コンテンツ鍵Kcで復号可能な暗号化が施される。コンテンツ鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータE(Kc, Dc)が、この形式でデジタル放送網により端末装置10のユーザに配布される。

なお、以下においては、E(X, Y)という表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。また、データDcに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Diが配布される。

20 また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスID(LID)が端末装置10を介してライセンス提供装置40とHD20との間でやり取りされる。さらに、ライセンスとしては、データDcおよびコンテンツ鍵Kcを識別するためのコードであるデータID(DID)や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ACが存在する。

コンテンツ鍵K<sub>c</sub>と、制御情報A<sub>C</sub>と、D<sub>ID</sub>と、L<sub>ID</sub>とを併せて、以後、ライセンスL<sub>IC</sub>と総称することとする。D<sub>ID</sub>は、データD<sub>c</sub>とコンテンツ鍵K<sub>c</sub>との対にして割り当てられた識別情報、すなわち、暗号化データE（K<sub>c</sub>，D<sub>c</sub>）を識別するための識別情報となる。D<sub>ID</sub>は、ライセンスL<sub>IC</sub>の他に、  
5 暗号化データE（K<sub>c</sub>，D<sub>c</sub>）とともに常に扱われる付加情報D<sub>i</sub>にも含まれ、参照できるようになっている。

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

HD 20などのデータ記憶装置および端末装置10などに備えられる再生回路には、固有のクラス公開鍵K<sub>P c m y</sub>およびK<sub>P c p y</sub>がそれぞれ設けられ、クラス公開鍵K<sub>P c m y</sub>およびK<sub>P c p y</sub>は、データ記憶装置に固有のクラス秘密鍵K<sub>c m y</sub>および再生回路に固有のクラス秘密鍵K<sub>c p y</sub>によってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「y」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。  
10  
15

また、データ記憶装置のクラス証明書としてC<sub>m y</sub>が設けられ、再生回路のクラス証明書としてC<sub>p y</sub>が設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。  
20

データ記憶装置のクラス証明書C<sub>m y</sub>は、K<sub>P c m y</sub>//I<sub>c m y</sub>//E（K<sub>a</sub>，H（K<sub>P c m y</sub>//I<sub>c m y</sub>））の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書C<sub>p y</sub>は、K<sub>P c p y</sub>//I<sub>c p y</sub>//E（K<sub>a</sub>，H（K<sub>P c p y</sub>//I<sub>c p y</sub>））の形式で出荷時に再生回路に記憶される。ここで、X//Yは、XとYとの連結を表わし、H（X）は、ハッシュ関数により演算されたデータXのハッシュ値を表わす。マスタ鍵K<sub>a</sub>は、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報I<sub>c m y</sub>，I<sub>c p y</sub>は、クラスごとの機器に関する情報およびクラス公  
25

開鍵を含む情報データである。

また、 $E(Ka, H(KPcmy//Icmy))$  および $E(Ka, H(KPcmy//Icmy//Icmy))$  は、それぞれ $KPcmy//Icmy$  および $KPcmy//Icmy//Icmy$  に対する電子署名を行なった署名データである。

5 なお、認証局は、署名データを作成する公的な第三者機関であり、署名データ $E(Ka, H(KPcmy//Icmy))$  および $E(Ka, H(KPcmy//Icmy//Icmy))$  は、認証局によって生成される。

さらに、データ記憶装置に対して安全かつ確実にライセンス L I C を送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵 $KPomz$  と、個別公開鍵 $KPomz$  で暗号化されたデータを復号することが可能な個別秘密鍵 $Komz$  とが存在する。ここで、記号「 $z$ 」は、データ記憶装置を個別に識別するための識別子である。

10 データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置 40、データ記憶装置 (HD 20) 、および端末装置 10 の再生回路において生成されるセッション鍵 $Ks1x, Ks2x$  が用いられる。

15 ここで、セッション鍵 $Ks1x, Ks2x$  は、ライセンス提供装置 40、データ記憶装置 (HD 20) 、もしくは端末装置 10 の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。

20 「セッション」には、ライセンス提供装置 40 からデータ記憶装置 (HD 20) へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置 (HD 20) から端末装置 10 の再生回路へライセンスを出力する「再生許諾セッション」がある。

25 これらのセッション鍵 $Ks1x, Ks2x$  は、各セッションごとに固有の値を有することにより、ライセンス提供装置 40、データ記憶装置 (HD 20) 、および端末装置 10 の再生回路によって管理される。具体的には、セッション鍵 $Ks1x$  は、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵 $Ks2x$  は、ライセンスの受信側によってセッションごとに発生される。なお、記号「 $x$ 」は、セッションにおける一連の処理

5 を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスLIC、またはコンテンツ鍵を含むライセンスLICの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

図4は、図1に示したライセンス提供装置40の構成を示す概略ブロック図である。

10 ライセンス提供装置40は、管理対象のライセンスを保持するデータベースであるコンテンツDB402と、ライセンスを配信する配信セッションにおける全ての通信記録を隨時記憶し、保持するデータベースであるログDB404と、コンテンツDB402およびログDB404とバスBS1を介してデータをやり取りし、所定の処理を行なうためのデータ処理部410と、ネットワーク30を介して端末装置10とデータ処理部410との間でデータ授受を行なうための通信装置450とを備える。

15 データ処理部410は、バスBS1上のデータに応じて、データ処理部410の動作を制御するための配信制御部412と、配信制御部412により制御されて、配信セッション時にセッション鍵K<sub>s1x</sub>を発生するためのセッション鍵発生部414と、端末装置10から送られてくるHD20のクラス証明書C<sub>my</sub>に含まれる署名データE(K<sub>a</sub>, H(K<sub>Pcmy</sub>//I<sub>cmy</sub>))を復号するためのHD20の認証鍵K<sub>Pa</sub>を保持するK<sub>Pa</sub>保持部416と、HD20から送られてきたクラス証明書C<sub>my</sub>を通信装置450およびバスBS1を介して受け、K<sub>Pa</sub>保持部416から受ける認証鍵K<sub>Pa</sub>によって復号処理を行ない、クラス証明書C<sub>my</sub>に含まれる署名データE(K<sub>a</sub>, H(K<sub>Pcmy</sub>//I<sub>cmy</sub>))の復号処理と、クラス証明書C<sub>my</sub>に含まれるK<sub>Pcmy</sub>//I<sub>cmy</sub>のハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書C<sub>my</sub>の検証を行なう認証部418と、配信セッションごとに、セッション鍵発生部414により生成されたセッション鍵K<sub>s1x</sub>を認証部418によってクラス証明書C<sub>my</sub>から抽出したクラス公開鍵K<sub>Pcmy</sub>を用いて暗号化し、バスBS1に出力するための暗号処理部420と、セッション鍵K<sub>s1x</sub>によって暗号化された上で

送信されたデータをバスBS1より受け、復号処理を行なう復号処理部422とを含む。

データ処理部410は、さらに、配信制御部412から与えられるライセンスLICを、復号処理部422によって得られたデータ記憶装置ごとに固有な個別公開鍵K<sub>P o m z</sub>によって暗号化するための暗号処理部424と、暗号処理部424の出力を、復号処理部422から与えられるセッション鍵K<sub>s 2 x</sub>によってさらに暗号化してバスBS1に出力するための暗号処理部426とを含む。

なお、個別公開鍵K<sub>P o m z</sub>およびセッション鍵K<sub>s 2 x</sub>は、セッション鍵K<sub>s 1 x</sub>によって暗号化されたうえで端末装置10から提供される。復号処理部422は、これを復号して個別公開鍵K<sub>P o m z</sub>を得る。

ライセンス提供装置40の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図5は、図1に示した端末装置10の構成を説明するための概略ブロック図である。

端末装置10は、デジタル放送網によって伝送される信号を受信するアンテナ102と、アンテナ102からの信号を復調してデータに変換、あるいはアンテナ102から送信するデータを変調してアンテナ102に与える受信部104と、端末装置10をネットワーク30に接続するモデム106と、端末装置10の各部のデータ授受を行なうバスBS2と、バスBS2を介して端末装置10の動作を制御するコントローラ108と、HD20とバスBS2との間のデータの授受を制御するHDインターフェース部110とを含む。

端末装置10は、さらに、上述したクラス証明書C<sub>p y</sub>を保持する認証データ保持部1502を含む。ここで、端末装置10のクラスを識別する識別子yは、y=3であるとする。

端末装置10は、さらに、クラス固有の復号鍵であるクラス秘密鍵K<sub>c p 3</sub>を保持するK<sub>c p</sub>保持部1504と、バスBS2から受けたデータをクラス秘密鍵K<sub>c p 3</sub>によって復号し、HD20によって発生されたセッション鍵K<sub>s 1 x</sub>を得る復号処理部1506とを含む。

端末装置10は、さらに、HD20に記憶されたコンテンツデータの再生を行

なう再生許諾セッションにおいて、HD 20との間でやり取りされるデータを暗号化するためのセッション鍵K<sub>s 2 x</sub>を乱数等により発生するセッション鍵発生部1508と、HD 20からコンテンツ鍵K<sub>c</sub>を受取る際に、セッション鍵発生部1508により発生されたセッション鍵K<sub>s 2 x</sub>を復号処理部1506によつて得られたセッション鍵K<sub>s 1 x</sub>によって暗号化し、バスBS2に出力する暗号処理部1510と、バスBS2上のデータをセッション鍵K<sub>s 2 x</sub>によって復号して、コンテンツ鍵K<sub>c</sub>を出力する復号処理部1512と、バスBS2より暗号化コンテンツデータE (K<sub>c</sub>, D<sub>c</sub>) を受けて、復号処理部1512からのコンテンツ鍵K<sub>c</sub>によって暗号化コンテンツデータE (K<sub>c</sub>, D<sub>c</sub>) を復号してデータD<sub>c</sub>を再生部1516へ出力する復号処理部1514と、復号処理部1514からの出力を受けてコンテンツを再生するための再生部1516と、再生部1516の出力をデジタル信号からアナログ信号に変換するDA変換部1518と、DA変換部1518の出力をテレビモニターなどの外部出力装置（図示省略）へ出力するための端子1520とを含む。

なお、図5においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路150を構成する。再生回路150は、セキュリティを向上させるために1チップ構成の半導体デバイスであることが好ましい。さらには、再生回路150は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

端末装置10の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

ここでは、端末装置10は、暗号化コンテンツデータを受信する機能、ライセンスの配信を受ける機能、再生許諾によって暗号化コンテンツデータを再生する機能を備えていたが、HD 20が端末装置10から脱着可能なデータ記憶装置であることから明らかのように、これらの機能を別々の装置によって実現してもよい。この場合、目的とする機能を実現する装置にHD 20を装着することで容易に実現できる。

図6は、図1に示すHD 20の構成を説明するための概略ブロック図である。すでに説明したように、データ記憶装置であるHD 20には、クラス公開鍵K

$K_{Pcm_y}$  とクラス秘密鍵  $K_{cm_y}$  のペア、および個別公開鍵  $K_{Pom_z}$  と個別秘密鍵  $K_{om_z}$  のペアが設けられるが、HD 20においては、これらを識別する識別子  $y = 1$ 、識別子  $z = 2$  で表されるものとする。

したがって、HD 20は、クラス証明書  $Cm1$  として認証データ  $K_{Pcm1} / I_{cm1} // E (Ka, H (K_{Pcm1} // I_{cm1}))$  を保持する認証データ保持部 202 と、クラス秘密鍵  $K_{cm1}$  を保持する  $K_{cm}$  保持部 204 と、個別秘密鍵  $K_{om2}$  を保持する  $K_{om}$  保持部 206 と、個別秘密鍵  $K_{om2}$  によって復号可能な個別公開鍵  $K_{Pom2}$  を保持する  $K_{Pom}$  保持部 208 とを含む。

このように、データ記憶装置（ここではHD 20）の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をデータ記憶装置単位で実行することが可能になる。

HD 20は、さらに、端末装置 10 の HD インターフェース部 110 と端子 210 を介して信号を授受する ATA (A T - A t t a c h m e n t) インターフェース部 212 と、HD 20におけるデータ伝送路であるバス BS3 と、ATA インターフェース部 212 からコントローラ 214 を介してバス BS3 に出力されたデータを、 $K_{om}$  保持部 206 により与えられた個別秘密鍵  $K_{om2}$  により復号し、ライセンス提供装置 40 から配信されたライセンス L I C をセキュアデータ記憶部 250 へ出力する復号処理部 216 と、 $K_{Pa}$  保持部 218 から認証鍵  $K_{Pa}$  を受け、バス BS3 に出力されたデータの認証鍵  $K_{Pa}$  による復号処理を実行して復号結果をコントローラ 214 へ出力し、かつ、得られたクラス公開鍵  $K_{Pcm1}$  を暗号処理部 222 へ出力する認証部 220 と、切換スイッチ 260 によって選択的に与えられるセッション鍵  $K_{s1x}$  または  $K_{s2x}$  によって、切換スイッチ 262 によって選択的に与えられるデータを暗号化してバス BS3 に出力する暗号処理部 224 とを含む。

HD 20は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵  $K_{s1x}$ 、 $K_{s2x}$  を発生するセッション鍵発生部 226 と、セッション鍵発生部 226 の出力したセッション鍵  $K_{s1x}$  を認証部 220 によって得られる端末装置 10 の再生回路 150 のクラス公開鍵  $K_{PcPy}$  あるいは他のデータ記憶装置（HD 21 とする）のクラス公開鍵  $K_{Pcm_y}$  によって暗号

化してバスB S 3に送出する暗号処理部2 2 2と、バスB S 3よりセッション鍵K s 2 xによって暗号化されたデータを受けてセッション鍵発生部2 2 6より得たセッション鍵K s 1 xまたはK s 2 xによって復号する復号処理部2 2 8とを含む。

5 HD 2 0は、さらに、バスB S 3上のデータをクラス公開鍵K P c m 1と対をなすクラス秘密鍵K c m 1によって復号するための復号処理部2 3 0と、ライセンスL I CをHD 2 0からHD 2 1へ移動または複製するために出力する際に、提供先のHD 2 1から受信した個別公開鍵K P o m z (z ≠ 2)によりライセンスL I Cを暗号化する暗号処理部2 3 2とを含む。

10 HD 2 0は、さらに、暗号化コンテンツデータE (K c , D c)を再生するためのライセンスL I Cと、HD 2 0が処理しているセッションの処理記録であるログとをバスB S 3より受けて記憶するセキュアデータ記憶部2 5 0を含む。そして、ライセンスL I Cは、セキュアデータ記憶部2 5 0内のライセンス領域に格納され、ログは、セキュアデータ記憶部2 5 0内のログメモリに格納される。セキュアデータ記憶部2 5 0は、たとえば半導体メモリによって構成される。

図7は、セキュアデータ記憶部2 5 0におけるメモリ構成を示した図である。

図7を参照して、セキュアデータ記憶部2 5 0は、ライセンス領域2 5 1と、有効フラグ領域2 5 2と、ログメモリ2 5 3とを含む。

20 ライセンス領域2 5 1は、L個 (Lは自然数) の領域2 5 1 1～2 5 1 Lから成り、それぞれ1つのライセンス (コンテンツ鍵K c 、制御情報A C、ライセンスI D (L I D) 、データI D (D I D) ) を格納する。

25 領域2 5 1 1～2 5 1 Lに格納された複数のライセンスの各々は、アドレス (以下、L B A : L o g i c a l B l o c k A d d r e s sと称する。) によって管理される。そして、各セッションにおいて記憶あるいは読み出されるライセンスL I Cは、全てL B Aにより特定される。

領域2 5 1 1～2 5 1 Lに対応してm a x L B A + 1～m a x L B A + LのL B Aが付与されているものとする。たとえば、領域2 5 1 3に格納されたライセンスL I Cは、L B A : m a x L B A + 3によって特定される。このとき、L B A : 0～m a x L B Aは、ノーマルデータ記憶領域2 7 0に割り当てられるものと

する。詳細は後述する。

なお、ライセンス領域 251 には、ノーマルデータ記憶領域 270 に割当てられた LBA (0 ~ max LBA) に続く値、すなわち、 $max LBA + 1 \sim max LBA + L$  が LBA として割当てられると説明したが、ライセンス領域 251 に割当てる LBA を限定するものではない。ライセンス領域 251 に割当てた L 個の LBA によって、それぞれが領域 2511 ~ 251L のいずれか 1 つを指定できる値であればいかなる値であってもよく、ノーマルデータ記憶領域 270 に割当てた LBA と重複する値、あるいは、独立した値を LBA として割当てもよい。

10 また、有効フラグ領域 252 は、セキュアデータ記憶部 250 上の記憶位置を特定する LBA それぞれに対応して設けられ、対応する LBA によって特定される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

15 有効フラグ領域 252 は、領域 2521 ~ 252L から成り、領域 2521 ~ 252L は、それぞれ、対応する領域 2511 ~ 251L に格納されたライセンス LIC の”有効”、または”無効”を格納する。

20 有効フラグ領域 252 のフラグが”有効”であるとき、フラグに対応する LBA によって特定されるセキュアデータ記憶部 250 上の記憶位置に記憶されているライセンス LIC は利用可能であり、ユーザはそのライセンス LIC 内のコンテンツ鍵  $K_c$  を再生許諾によって読み出して、対応する暗号化コンテンツデータを復号し、コンテンツデータを再生したり、そのライセンス LIC を他のデータ記憶装置に移動・複製することができる。

一方、有効フラグ領域 252 のフラグが”無効”であるとき、そのフラグに対応する LBA によって特定されるセキュアデータ記憶部 250 上の記憶位置に記憶されているライセンス LIC は利用不可であり、HD20 のコントローラ 21 25 4 によって、その LBA からのライセンス LIC は拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンス LIC に対応したコンテンツデータを再生することはできない。この有効フラグ領域 252 のフラグは、ライセンスの新たな記憶によって”有効”とされ、ライセンスの移動によって”無効”とされる。

ログメモリ 253 は、ライセンスを HD 20 に入出力する場合の履歴情報（以下では「ログ」と呼ぶ。）を 1 つ格納する N（N は自然数）個の領域 2531～253N からなるリングメモリである。領域 2531～253N は、それぞれ、バンク 0～N-1 と称される領域を特定する名称が付与されている。したがって、  
5 バンク n（n は N の剩余系）とは、ログメモリ上の中の領域 253 (n-1) を示す。

ログメモリ 253 は、複数のログをリング状に格納する。すなわち、ログメモリ 253 は、バンク 0 によって特定される領域 2531 からログの格納を開始し、バンク N-1 によって特定される領域 253N にログを格納すると、再びバンク 0 によって特定される領域 2531 に戻り、ログを格納する。

10 バンク 0～N-1、すなわち、ログメモリ 253 の領域 2531～253N の各々に格納されるログは、管理番号領域 2541 と、ライセンス ID (LID) 領域 2542 と、Ks2x 領域 2543 と、ST1 領域 2544 と、ST2 領域 2545 と、KPCmy 領域 2546 と、LBA 領域 2547 とを含む。

15 管理番号領域 2541 は、ログをバンク 0～N-1 の各々に格納する際に、ログの格納の順序を示す管理番号を格納する。そして、管理番号は、M (M>N、M は自然数) の剩余系をなして、昇順に付与される。この管理番号を格納することによって、最新のログを格納した、あるいは、最も古いログを格納したバンクを検索することができるようになる。すなわち、最初に管理番号 1 のログがバンク 0 に格納されるとすると、そのログの管理番号領域 2541 は、管理番号”  
20 1”を格納する。そして、ライセンスの入出力に伴い、新たなログを格納するごとに、バンク 2 から順に使用し、そのログの管理番号領域 2541 に、新たなログを格納するバンクの直前のバンクに格納される最新のログの管理番号領域 2541 に格納される管理番号に 1 づつ増加した管理番号を格納する。したがって、各バンク 0～N-1、すなわち、領域 2531～253N に格納されたログの管理番号領域 2541 から管理番号を読み出せば、管理番号に基づいてそのログが新しいか古いかを判断できる。この判断は、次のようにして行なう。すなわち、連続する 2 つのバンク n, n+1 (n は N の剩余系) が保持する管理番号が不連続である場合、バンク n には最新のログが、バンク n+1 には最も古いログが保持されている。さらに、詳細な説明は、後述する。

以降では、特に断らない限り、管理番号に関する表記および演算は全てMの剩余系においてログメモリ253の領域2531～253Nを指定するバンクの番号に関する表記および演算は全てNの剩余系における表記および演算を示している。

5 ライセンスID領域2542は、セッションの対象となるライセンスLICを特定するライセンスID(LID)を格納する。Ks2x領域2543は、セッションにおいてライセンスLICの受信側のデータ記憶装置によって生成されたセッション鍵Ks2xを格納する。

10 ST1領域2544は、動作中のセッションにおける処理の状態を示すステータスST1を格納する。ST2領域2545は、ライセンスID領域2542に格納されるライセンスIDに対応したライセンスの記憶状態を示すステータスST2を格納する。

15 KPcmx領域2546は、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵KPCmxを格納する。LBA領域2547は、各セッションにおいてライセンスLICを読み出あるいは記憶するために指示されたLBAを格納する。

20 一連のセッションの処理が進行するにつれて、上記各領域のデータが更新あるいは参照されていく。ステータスST1は、”受信待”、”受信済”、”送信待”および”送信済”の4状態のいずれかであり、ステータスST2は、”データ有”、”データ無”および”移動済”の3状態のいずれかである。

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンスLICに対して、ログメモリ253内のライセンスID領域2541に格納されているライセンスIDと、LBA領域2547に格納されたLBAとによって当該ライセンスLICの記憶状態が確認され、その確認結果に応じてステータスST2が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ253内に格納されているライセンスLIC、セッション鍵Ks2x、ステータスST1およびステータスST2を受取って、自身が記録するログの内容と受取ったライセンスLIC、セッション鍵Ks2x、ステータスST1およ

びステータス S T 2 とを確認することにより、再度のライセンスの送信を行なつてもよいか否かの判断がされる。

なお、セッション鍵 K s 2 x は、各セッションを特定するために記憶され、セッション鍵 K s 2 x を共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

また、ステータス S T 2 には、出力ログが出力される際に、ログメモリ 2 5 3 に格納されているライセンス I D (L I D) と L B A とによってセキュアデータ記憶部 2 5 0 における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

再び図 6 を参照して、HD 2 0 のデータ記録部に関して説明する。HD 2 0 は、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部 2 7 0 を含む。ノーマルデータ記憶部 2 7 0 は、データが記憶される円盤状の磁気記録媒体 2 7 0 1 と、磁気記録媒体 2 7 0 1 を回転させるモータ 2 7 0 2 と、モータ 2 7 0 2 を制御するサーボ制御部 2 7 0 3 と、磁気記録媒体 2 7 0 1 上における磁気ヘッドの位置を制御するシーク制御部 2 7 0 4 と、磁気ヘッドヘデータの記録および再生を指示する記録再生処理部 2 7 0 5 とを含む。

HD 2 0 は、さらに、A T A インターフェース部 2 1 2 を介して外部との間でデータ授受、制御情報 A C に基づくライセンスの出力に関する判断、およびセキュアデータ記憶部 2 5 0 の管理などの HD 2 0 内の動作を制御するためのコントローラ 2 1 4 を含む。

なお、ノーマルデータ記憶部 2 7 0 、A T A インターフェース部 2 1 2 および端子 2 1 0 を除く他の構成は、耐タンパモジュール領域に構成される。

図 8 を参照して、ノーマルデータ記憶部 2 7 0 の構成は、一般の公知のハードディスクの構成と変わることろはなく、データ記憶部 2 7 0 0 を含む。データ記憶部 2 7 0 0 は、領域 2 8 0 0 ～ 2 8 0 A (A = m a x L B A 、 m a x L B A は自然数) の各々は、暗号化コンテンツデータおよび暗号化コンテンツデータの附属データ、ライセンステーブル等を格納する。そして、領域 2 8 0 0 ～ 2 8 0 A に対応して L B A : 0 ～ m a x L B A が付与されており、各領域 2 8 0 0 ～ 2 8

0 Aは、L B A : 0 ~ m a x L B Aによって指定され、暗号化コンテンツデータ等のデータは、指定された各領域2 8 0 0 ~ 2 8 0 Aに入出力される。

なお、ライセンステーブルは、暗号化コンテンツデータとライセンスの関係を示す情報テーブルであり、ライセンステーブルを参照することで、暗号化コンテンツデータに対応するライセンスと、そのライセンスが記憶されているL B Aを特定することができる。したがって、ライセンステーブルは、暗号化コンテンツデータの記憶、削除時、あるいはライセンスの記憶、移動、削除時にその内容が変更される。

したがって、H D 2 0は、L B A : 0 ~ m a x L B Aによって指定できるノーマルデータ記憶部2 7 0と、それに続くL B A : m a x L B A + 1 ~ m a x L B A + Lによって指定できるセキュアデータ記憶部2 5 0、より具体的には、ライセンスマモリ2 5 1に対してデータあるいはライセンスの入出力が行なうことができる。

また、ノーマルデータ記憶領域2 7 0およびライセンス領域2 5 1に対するL B Aの値については、本実施の形態に限るものではない。

なお、セキュアデータ記憶部2 5 0は、通常のアクセスコマンドではA T Aインターフェース部2 1 2を介して、直接、外部からアクセスできない等の手段を設けることで耐タンパ性を確保した、耐タンパ構造を備えている。

また、H D 2 0のセキュアデータ記憶部2 5 0は、全て半導体メモリによって構成されるものとして説明したが、耐タンパ性を確保した上で、セキュアデータ記憶部2 5 0の一部あるいはその全てを、磁気記録媒体2 7 0 1上に記憶する構成としてもよい。

以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

#### 25 [配信]

まず、図1に示すデータ配信システムにおいて、ライセンス提供装置4 0から端末装置1 0に装着されたH D 2 0へライセンスを配信する動作について説明する。

図9および図10は、図1に示すデータ配信システムにおいて、端末装置1 0

のユーザが端末装置10から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンスがライセンス提供装置40から端末装置10に装着されたHD20へ向けて送信され、HD20に記憶される際の処理（配信セッション）を説明するための第1および第2のフローチャートである。

5 図9における処理開始以前に、端末装置10のユーザは、端末装置10をモデム106によりネットワーク30に接続し、端末装置10をネットワーク30を介してライセンス提供装置40に接続していることを前提としている。

10 図9を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置10のコントローラ108は、バスB S 2およびHDインターフェース部110を介してHD20へクラス証明書の出力要求を出力する（ステップS1）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してクラス証明書の出力要求を受理すると（ステップS2）、バスB S 3を介して認証データ保持部202からクラス証明書Cm1=K P c m 1 // I c m 1 // E (K a, H (K P c m 1 // I c m 1))を読み出し、クラス証明書Cm1をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS3）。

20 端末装置10のコントローラ108は、HD20からHDインターフェース部110およびバスB S 2を介してクラス証明書Cm1を受理すると（ステップS4）、受理したクラス証明書Cm1をモデム106およびネットワーク30を介してライセンス提供装置40へ送信する（ステップS5）。

ライセンス提供装置40では、端末装置10からクラス証明書Cm1を受信すると（ステップS6）、受信したCm1が正当なクラス証明書であるか否かを認証する（ステップS7）。認証処理は次のように行なわれる。

25 ライセンス提供装置40は、クラス証明書Cm1=K P c m 1 // I c m 1 // E (K a, H (K P c m 1 // I c m 1))を受理すると、HD20から出力されたクラス証明書Cm1に含まれる署名データE (K a, H (K P c m 1 // I c m 1))を認証部418において認証鍵K P aで復号し、ハッシュ値H (K P m 1 // I c m 1)を抽出する。そして、さらに、認証部418は、クラス証

明書Cm1に含まれるK P c m 1 // I c m 1のハッシュ値を演算し、クラス証明書Cm1から抽出したハッシュ値と演算したハッシュ値とを比較する。配信制御部412は、認証部418における復号処理結果から、上記の復号ができ、かつ、2つのハッシュ値の値が一致したと判断すると、HD20から受理したクラス証明書Cm1は、正当な証明書であると判断する。

5 ステップS7において、クラス証明書Cm1が正当な証明書であると判断された場合、配信制御部418は、クラス公開鍵K P c m 1を受理する（ステップS8）。そして、次の処理（ステップS9）へ移行する。正当なクラス証明書でない場合には、クラス証明書Cm1を受理しないでエラー通知を端末装置10へ出力し（図10のステップS44）、端末装置10においてエラー通知が受理されると（図10のステップS45）、配信セッションが終了する。

10 ステップS8においてクラス公開鍵K P c m 1が受理されると、配信制御部412は、ライセンスID（LID）を生成し（ステップS9）、さらに制御情報ACを生成する（ステップS10）。そして、セッション鍵発生部414は、配信のためのセッション鍵K s 1 aを生成する（ステップS11）。セッション鍵K s 1 aは、認証部418によって得られたHD20に対応するクラス公開鍵K P c m 1によって、暗号処理部420によって暗号化され、暗号データE（K P c m 1, K s 1 a）が生成される（ステップS12）。

15 そして、配信制御部412は、ライセンスID（LID）および暗号化されたセッション鍵K s 1 aを1つのデータ列LID//E（K P c m 1, K s 1 a）として、バスBS1および通信装置450を介して端末装置10へ向けて出力する（ステップS13）。

20 端末装置10は、ネットワーク30を介してLID//E（K P c m 1, K s 1 a）を受信すると（ステップS14）、受信したLID//E（K P c m 1, K s 1 a）をHD20へ出力する（ステップS15）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E（K P c m 1, K s 1 a）を受理する（ステップS16）。コントローラ214は、バスBS3を介して受理したE（K P c m 1, K s 1 a）を復号処理部230へ与え、復号処理部230は、K c m保持部204に保持される

HD 2 0 に固有なクラス秘密鍵K c m 1 によって復号処理することにより、セッション鍵K s 1 a を復号し、セッション鍵K s 1 a を受理する（ステップS 1 7）。

HD 2 0 のコントローラ2 1 4 は、ライセンス提供装置4 0 で生成されたセッション鍵K s 1 a の受理を確認すると、ATAインターフェース部2 1 2 および端子2 1 0 を介してその旨を端末装置1 0 に通知する。端末装置1 0 のコントローラ1 0 8 は、HDインターフェース部1 1 0 およびバスB S 2 を介して、HD 2 0 においてセッション鍵K s 1 a が受理された旨の通知を受理すると、HD 2 0 にセッション鍵の生成の要求通知をバスB S 2 およびHDインターフェース部1 1 0 を介してHD 2 0 へ出力する（ステップS 1 8）。HD 2 0 のコントローラ2 1 4 は、端子2 1 0 およびATAコントローラ2 1 2 を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部2 2 6 に対してセッション鍵の生成を指示する。そして、セッション鍵発生部2 2 6 は、セッション鍵K s 2 a を生成する（ステップS 1 9）。

そして、コントローラ2 1 4 は、セキュアデータ記憶部2 5 0 のログメモリ2 5 3 から最も古いをログが格納されているバンクを検索し、その検索したバンクn ( $0 \leq n \leq N - 1$ ) の管理番号領域2 5 4 1、ライセンスID領域2 5 4 2、K s 2 a 領域2 5 4 3、ST 1 領域2 5 4 4 に対して、それぞれ、新たな管理番号、ステップS 1 6 で受理したライセンスID、ステップS 1 9 において生成されたセッション鍵K s 2 a 、および”受信待”を格納する（ステップS 2 0）。したがって、バンクn に格納されるログは最も新しいログとなる。このとき、ログを構成する他の領域については、その内容を初期化、たとえば、全て”0”としてもよいし、そのままの状態であってもよい。

ここで、図1 1 を参照して、ステップS 2 0 の詳細な動作について説明する。図1 1 は、ステップS 2 0 の詳細な動作を示すフローチャートである。コントローラ2 1 4 は、ステップS 1 9 の後、ログメモリ2 5 3 のうち、最新のログが記録されているログ領域に対応するバンクn - 1 を特定し、そのバンクn - 1 によって指定されるログ領域に格納された履歴情報に含まれる管理番号m を取得する（ステップS 2 0 a）。

図12を参照して、ステップS20aの詳細な動作について説明する。図12は、ステップS20のさらに詳細なフローチャートである。コントローラ214は、ステップS19の後、変数nに対して領域2532を示すバンク1のバンク番号1を設定し（ステップS20c）、バンク0に格納されている管理番号を取得して、変数mに代入する（ステップS20d）。そして、コントローラ214は、ログメモリ253のバンクnに格納されている管理番号を取得して、変数m aに代入する（ステップS20e）、ma-mを演算して演算結果が”1”であるか否かを判定する（ステップS20f）。演算結果が”1”であるとき、コントローラ214は、変数nに、1を加えたn+1を代入し（ステップS20g）、変数maに代入されている管理番号を変数mに代入する（ステップS20h）。その後、ステップS20e～S20hが繰返し行なわれる。

ステップS20fにおいて、コントローラ214は、演算結果が”1”でないとき、バンクn-1が、最新のログが記録されている領域であると判断し、最新の管理番号mの取得を終了し、図11に示すステップS20bへ移行する。このとき、最も古いログはバンクnに格納されている。

ステップS20fにおいて、演算結果が”1”であると判定された場合に、ステップS20g、S20h、S20e、S20fが、順次、行なわれるは、演算結果が”1”である場合、変数mと変数maとに代入された管理番号mと管理番号maとが連続した番号であり、バンクn-1とバンクnとに、前後してログが格納されたことを示している。つまり、ログメモリ253の領域はバンク番号順に巡回的に使用され、かつ、管理番号もMの剩余系において巡回的に使用されるのであるから連続して格納された場合、連続するバンクに格納された管理番号の差は”1”となるからである。したがって、バンクn-1には、最新のログが格納されていないことが判る。なお、バンクnについては不明である。そして、判断する領域を1つ進めて、バンクnに格納されているログについて判定する。すなわち、バンクnに格納されているログの管理と、次の領域であるバンクn+1に格納されているログの管理番号に基づいて判定する。フローチャートでは、ステップS20gにおいて、nにはn+1が代入されることで次の領域に対する判定となる。

このように、ステップS 20 f, S 20 g, S 20 h, S 20 eのループを繰返し行なうことによってバンク0から順にバンクN-1まで連続した領域に格納された管理番号が連続しているか否かが判定される。なお、バンクN-1と比較されるのはバンク0の番号である、上述したように、バンクの番号に対する演算はNの剩余系においてなされる。すなわち、バンクN-1の判定においては、 $n - 1 = N - 1$ 、 $n = 0$ である。

ステップS 20 fにおいて、演算結果が”1”でない場合に、バンクn-1に格納されたログを最新のログと判定するのは、この場合、バンクn-1およびバンクnに格納される2つのログの管理番号が不連続であるからである。すなわち、上述したように、前後してログの管理番号は連続する。逆に連続しない管理番号を含むログは連続しないこととなる。

また、図12に従ってバンクn-1を特定するためには、HD20の出荷時ににおけるログメモリ253の初期化によってログメモリ253の全ての領域253 1～253 Nに、すなわち、バンク0～バンクN-1に対して、所定の管理番号を含むログを格納しておく必要がある。管理番号として全てのバンクに対して同じ値、あるいは、連続するバンクに連続する値（一ヶ所不連続となる）を持つログを格納しておく。なお、ログの他の領域については、いずれの値であってもよい。

再び、図11を参照して、上述した方法によって最新の履歴情報（ログ）が記録されているバンクn-1と、バンクn-1に格納された管理番号mとを取得した後、コントローラ214は、バンクnに、管理番号m+1、ステップS16で受理したライセンスID、ステップS19で受理したセッション鍵Ks2aを格納し、ST1領域2545のステータスST1を”受信待”に設定する（ステップS20b）。これにより、図9に示すステップS20の動作が終了し、ステップS21へ移行する。

再び、図9を参照して、ステップS20の後、暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1aによって、切換スイッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵Ks2aと個別公開鍵Kpom2とからなる1つ

のデータ列を暗号化し、E (Ks1a, Ks2a//KPom2) 生成する（ステップS21）。そして、暗号処理部224は、E (Ks1a, Ks2a//KPom2) をバスBS3に出力する。バスBS3に出力された暗号化データE (Ks1a, Ks2a//KPom2) は、コントローラ214により受理され、  
5 コントローラ214は、受理した暗号化データとライセンスID (LID) とを1つのデータ列としたデータLID//E (Ks1a, Ks2a//KPom2) をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS22）。

そして、端末装置10は、データLID//E (Ks1a, Ks2a//KPom2) をHD20から受理すると（ステップS23）、受理したデータをネットワーク30を介してライセンス提供装置40に出力する（ステップS24）。

ライセンス提供装置40は、データLID//E (Ks1a, Ks2a//KPom2) を受信すると（ステップS25）、復号処理部422においてセッション鍵Ks1aによる復号処理を実行し、HD20で生成されたセッション鍵Ks2a、およびHD20の個別公開鍵KPom2を受理する（ステップS26）。

配信制御部412は、ライセンスID (LID) に対応するデータID (DID) およびコンテンツ鍵KcをコンテンツDB402から取得し（ステップS27）、ライセンスID (LID) および制御情報ACと併せた1つのデータ列としてのライセンスLIC=Kc//AC//DID//LIDを生成する。

配信制御部412は、生成したライセンスLICを暗号処理部424に与える。暗号処理部424は、復号処理部422によって得られたHD20の個別公開鍵KPom2によってライセンスLICを暗号化して暗号化データE (KPom2, LIC) を生成する（ステップS28）。そして、暗号処理部426は、暗号処理部424から受ける暗号化データE (KPom2, LIC) を、復号処理部422から受けるセッション鍵Ks2aによって暗号化し、暗号化データE (Ks2a, E (KPom2, LIC)) を生成する（ステップS29）。

図10を参照して、配信制御部412は、バスBS1および通信装置450を介して暗号化データE (Ks2a, E (KPom2, LIC)) を端末装置10へ向けて出力する（ステップS30）。端末装置10は、ネットワーク30を介

して暗号化データE (Ks2a, E (Kpom2, LIC)) を受理すると (ステップS31) 、受理した暗号化データをHD20へ出力する (ステップS32) 。

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE (Ks2a, E (Kpom2, LIC)) を受理すると (ステップS33) 、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE (Ks2a, E (Kpom2, LIC)) を復号し、HD20において、ライセンスLICが個別公開鍵Kpom2により暗号化された暗号化ライセンスE (Kpom2, LIC) が受理される (ステップS34) 。

そして、復号処理部228は、暗号化ライセンスE (Kpom2, LIC) をバスBS3へ出力する。

コントローラ214の指示によって、暗号化ライセンスE (Kpom2, LIC) は、復号処理部216において個別秘密鍵Kom2によって復号され、ライセンスLICが受理される (ステップS35) 。

HD20のコントローラ214は、ライセンスLICの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてライセンスLICが受理された旨の通知を受理すると、HD20のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBA (「格納LBA」と呼ぶ。) をバスBS2およびHDインターフェース110を介してHD20へ出力する (ステップS36) 。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してライセンスLICの格納LBAを受理すると (ステップS37) 、その受理した格納LBAをログメモリ253のバンクnに格納されたログのLBA領域2547に記憶する (ステップS38) 。

そして、コントローラ214は、受理したライセンスLICに含まれるライセンスID (LID) と、ステップS16において受理したライセンスLID (LID) とを比較し、一致しているか否かをチェックする (ステップS39) 。コ

ントローラ 214 は、LID が一致しており、受理したライセンス LIC が正しいものであると判断すると、端末装置 10 から受理したセキュアデータ記憶部 250 内の LBA に、受理したライセンス LIC を記憶する（ステップ S40）。

コントローラ 214 は、指定された LBA にライセンス LIC を記憶すると、  
5 有効フラグ領域 252 のその LBA に対応するフラグを”有効”にする（ステップ S41）。そして、コントローラ 214 は、さらに、ログメモリ 253 のバンク n に格納されたログの ST1 領域 2544 のステータス ST1 を”受信済”に変更し（ステップ S42）、配信セッションにおける一連の処理が終了したことを端末装置 10 に通知する。

10 そして、端末装置 10 において、HD20 から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

一方、ステップ S39 において、コントローラ 214 は、LID が一致せず、受理したライセンス LIC が正しくないと判断すると、エラー通知を端末装置 10 へ出力し（ステップ S43）、端末装置 10 は、エラー通知を受理すると（ステップ S45）、処理を終了する。

図 9 および図 10 に示された配信処理においては、ライセンス提供装置 40 におけるログの記録に関する記載がなされていないが、図 4 に示すように、ライセンス提供装置 40 には、十分な記憶容量を持つログ DB404 が備えられており、配信セッションにおける各ステップにおけるログがログ DB404 に記憶される。  
20 また、ログ DB404 には、ライセンスの送信に伴なう課金情報なども記憶される。

図 9 および図 10 に示された配信処理における一連の処理において、ステップ S25 からステップ S44 の処理中に異常が発生して処理が中断したときは、再書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置 10 の電源が遮断されたり、ライセンス提供装置 40 側の異常、あるいは端末装置 10 とライセンス提供装置 40 との通信異常など、種々の異常ケースが考えられる。ここで、HD20 内のログメモリ 253 に格納されたステータス ST2 を除く出力ログの内容がすべて格納されたステップ S22 終了後からステップ S44 までの処理中に処理が中断した場合には、HD20 は、再書込処理を行なってラ

イセンスの提供を受けることが可能である。ここでは、端末装置 10 の判断によって再書き込み処理を行なうものとしたため、端末装置 10 において処理の進行が確認できるステップ S 22 からステップ S 24 を除く、ステップ S 25 からステップ S 44 の処理中に処理が中断した場合を再書き込み処理の対象とし、他のステップ 5 における処理の中断においてはライセンス提供装置 40 からライセンスの提供がなされなかつたものと判断し、図 9 および図 10 に示したフローチャートに従つて、最初から処理を行なうこととした。

同様に、ライセンス提供装置 40 がライセンスを出力するまでのライセンス提供装置 40 内のステップ S 25 からステップ S 30 までの処理については、端末装置 10 において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書き込み処理の対象から除外して、図 9 および図 10 に示したフローチャートにしたがつて、最初から処理を行なうものとしてもよい。

#### [配信における再書き込み]

図 13～図 15 は、図 9 および図 10 において示した配信処理におけるステップ S 25 からステップ S 44 の処理中に異常が発生したときに行なわれる再書き込み処理の第 1 から第 3 のフローチャートであり、図 16 は、図 13 のステップ S 1\_12a の詳細な動作を説明するためのフローチャートである。

図 13 を参照して、端末装置 10 は、ステップ S 25 からステップ S 44 の処理中に異常が発生したと判断すると、ライセンス L I C の L I D // 再書き込み要求をネットワーク 30 を介してライセンス提供装置 40 へ出力する（ステップ S 1\_01）。配信制御部 412 は、通信装置 450 およびバス B S 1 を介して L I D // 再書き込み要求を受理すると（ステップ S 1\_02）、セッション鍵発生部 414 にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部 414 は、再書き込み処理のためのセッションキー鍵 K s 1b を生成する（ステップ S 1\_03）。そして、配信制御部 412 は、このセッションにおいて HD 20 とやり取りしたログが格納されているログ D B 402 から HD 20 に対応するクラス公開鍵 K P c m 1 を取得し（ステップ S 1\_04）、暗号処理部 420 に与える。クラス公開鍵 K P c m 1 を受けた暗号処理部 420 は、クラス公開鍵 K P c m 1 をによりセッション鍵 K s 1b を暗号化し、E (K P c m 1, K s 1b) が生成

される（ステップS105）。そして、配信制御部412は、LID//E（K<sub>Pcm1</sub>, K<sub>s1b</sub>）をバスBS1および通信装置450を介して端末装置10へ向けて出力する（ステップS106）。

端末装置10は、ネットワーク30を介してLID//E（K<sub>Pcm1</sub>, K<sub>s1b</sub>）を受理すると（ステップS107）、受理したLID//E（K<sub>Pcm1</sub>, K<sub>s1b</sub>）をHD20へ出力する（ステップS108）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E（K<sub>Pcm1</sub>, K<sub>s1b</sub>）を受理する（ステップS109）。コントローラ214は、受理したE（K<sub>Pcm1</sub>, K<sub>s1b</sub>）をバスBS3を介して復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持されるHD20に固有なクラス秘密鍵K<sub>cm1</sub>によって復号処理することにより、セッション鍵K<sub>s1b</sub>を復号し、セッション鍵K<sub>s1b</sub>が受理される（ステップS110）。

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵K<sub>s1b</sub>の受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵K<sub>s1b</sub>が受理された旨の通知を受理すると、ログの出力要求をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS111）。

HD20のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理し（ステップS112）、ログの複製処理を行なう（ステップS112a）。

ここで、図16を参照して、ステップS112aの詳細な動作について説明する。コントローラ214は、ログメモリ253のうち、最新のログが格納されたバンクn-1の特定と、バンクn-1に格納されているログの管理番号mとを取得する（ステップS112b）。このステップS112bの詳細な動作は、図11および図12に示すフローチャートに従って行なわれる。

ステップS112bの後、コントローラ214は、変数k（kは自然数、1≤

5  $k \leq N$  ) に” 1 ” を、変数 E R R に” 偽 ” を代入し (ステップ S 1 1 2 c ) 、バンク  $n - k$  に格納されたログのライセンス I D ( L I D ) が、ステップ S 1 0 9 で受理したライセンス I D ( L I D ) に一致するか否かを判定する。すなわち、コントローラ 2 1 4 は、ステップ S 1 1 2 b で検出した最新のログに格納されたライセンス I D ( L I D ) が、ステップ S 1 0 9 で受理したライセンス I D ( L I D ) に一致するか否かを判定する。

10 2 つのライセンス I D ( L I D ) が不一致である場合、コントローラ 2 1 4 は、  $k$  が  $N$  ( バンクの総数 ) よりも小さいか否かを判定し (ステップ S 1 1 2 e ) 、  $k$  が  $N$  以上であるとき、全てのバンクに対して確認が終了し、つまり、受理したライセンス I D ( L I D ) に一致する L I D を記録したログが格納されていないことが確認され、ステップ S 1 1 2 h へ進み、変数 E R R に” 真 ” を代入する (ステップ S 1 1 2 h ) 。そして、図 1 3 のステップ S 1 1 3 a に戻り、変数 E R R を確認する。

15 再び、図 1 3 を参照して、コントローラ 2 1 4 は、変数 E R R を確認する (ステップ S 1 1 3 a ) 。図 1 6 のステップ S 1 1 2 h から移行した場合、変数 E R R は” 真 ” であり、該当するライセンス I D を記録するログが、ログメモリ 2 5 3 に格納されていなかったことを示しているので処理を継続することはできない。したがって、図 1 5 に示すステップ S 1 6 0 へ移行し、エラー通知を端末装置 1 0 へ出力する (ステップ S 1 6 0 ) 。そして、端末装置 1 0 は、エラー通知を受 20 理し (ステップ S 1 6 1 ) 、書込拒否により一連の動作が終了する。

25 図 1 6 を参照して、ステップ S 1 1 2 e において、コントローラ 2 1 4 は、  $k$  は  $N$  よりも小さいと判定すると、全てのバンクに対する確認が終了していないので、今、確認したログより、1 つ古いログを確認するために、変数  $k$  に  $k - 1$  を代入する (ステップ S 1 1 2 f ) 、ステップ S 1 1 2 d へ移行する。そして、コントローラ 2 1 4 は、バンク  $n - k$  に格納されたライセンス I D ( L I D ) が、ステップ S 1 0 9 で受理したライセンス I D ( L I D ) と一致するか否かを判定する。この場合、変数  $k$  の値は” 2 ” であるので、コントローラ 2 1 4 は、バンク  $n - 2$  に格納されたログのライセンス I D ( L I D ) が、ステップ S 1 0 9 で受理したライセンス I D ( L I D ) に一致するか否かを判定する。そして、2 つ

のライセンス I D (L I D) が不一致である場合、ステップ S 1 1 2 e, S 1 1 2 f, S 1 1 2 d が行なわれる。

このように、コントローラ 2 1 4 は、最新のログから、より古いログが格納されるバンクへ向けて、各バンクに格納されたライセンス I D (L I D) が、ステップ S 1 0 9 で受理したライセンス I D (L I D) と一致するか否かを判定する。そして、この動作（ステップ S 1 1 2 e, S 1 1 2 f, S 1 1 2 d）は、ステップ S 1 0 9 で受理したライセンス I D (L I D) に一致するライセンス I D (L I D) が検出されるまで、あるいは、全てのバンクの確認が終了するまで繰返し行なわれる。なお、バンク番号は N の剩余系であるので、ライセンス I D の確認は、バンク  $n-1$  ( $k=1$ ),  $n-2$  ( $k=2$ ), …,  $1$  ( $k=n-1$ ),  $0$  ( $k=n$ ),  $N-1$  ( $k=n+1$ ), …,  $n$  ( $k=N$ ) の順に確認される。

ステップ S 1 1 2 d において、2 つのライセンス I D (L I D) が一致したとき、コントローラ 2 1 4 は、バンク  $n-k$  に格納されたログを取得し、その取得したログの管理番号 m を  $m+1$  に変更した後、そのログをバンク n に格納する（ステップ S 1 1 2 g）。つまり、コントローラ 2 1 4 は、ライセンス提供装置 4 0 から送信されたライセンス I D (L I D) に一致するライセンス I D (L I D) を含むログがログメモリ 2 5 3 に格納されている場合、そのログ（複数有る場合は、より新しいログ）を、最も古いログが格納されたバンク n に複製する。この場合、管理番号のみは複製されず、複製したログが新しいログとして扱われるよう先のバンク  $n-1$  に格納されたログの管理番号に 1 を加えた値を記録する。したがって、最も古いログは削除され、そこに、現在、進行中の再書き込み処理に対する新たなログが格納される。

その後、図 1 3 に示すステップ S 1 1 3 a へ移行する。

再び、図 1 3 を参照して、コントローラ 2 1 4 は、変数 E R R を格納する（ステップ S 1 3 3 a）。図 1 6 に示すステップ S 1 1 2 g から移行した場合、変数 E R R は”偽”であり、該当するライセンス I D を記録したログがバンク n に複製されるので処理の継続が可能であると判断され、ステップ S 1 1 3 へ移行して、ログメモリ 2 5 3 のバンク n に格納された格納 L B A に記憶されるライセンス L I C のライセンス I D (L I D) と、ログメモリ 2 5 3 に格納されたライセンス

I D (L I D) とが一致するか否かをチェックする (ステップ S 1 1 3)。

コントローラ 2 1 4 は、両ライセンス I D (L I D) が一致すると判断すると、配信処理としては、ライセンス提供装置 4 0 からのライセンス L I C の受理まで 5 は行なわれ、HD 2 0 においてライセンス L I C は受理していると認識する。そ うすると、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n に格納された格 納 L B A により指定された領域に記憶されるライセンスに対応する有効フラグ領 域 2 5 2 に格納されているフラグをチェックして、そのライセンスの有効性をチ ェックする (ステップ S 1 1 4)。

コントローラ 2 1 4 は、ライセンスが有効であると判断すると、ログメモリ 2 10 5 3 のバンク n に格納されたログのステータス S T 2 を”データ有”に変更し、 次の処理 (ステップ S 1 1 8) へ移行する。一方、コントローラ 2 1 4 は、ステ ップ S 1 1 4 においてライセンスが無効であると判断すると、ログメモリ 2 5 3 のバンク n に格納されたログのステータス S T 2 を”移動済”に変更し、次の処 理 (ステップ S 1 1 8) へ移行する。

15 ステップ 1 1 3 において、コントローラ 2 1 4 は、比較したライセンス I D (L I D) が一致しないと判断したときは、ログメモリ 2 5 3 のバンク n に格納 されたログのステータス S T 2 を”データ無”に変更する (ステップ S 1 1 7)。

ステータス S T 2 の変更処理がなされると、コントローラ 2 1 4 は、ログメモ リ 2 5 3 のバンク n からライセンス I D (L I D) 、ステータス S T 1 , S T 2 20 およびセッション鍵 K s 2 c を取得する (ステップ S 1 1 8)。ここで、この処 理は図 9 および図 1 0 のフローチャートに従って配信セッションの中止に対する 処理であるためログメモリ 2 5 3 のバンク n に格納されているセッション鍵は K s 2 a であるが、説明の関係上、ログメモリ 2 5 3 のバンク n から取得したセッ ション鍵を K s 2 c としている。そして、コントローラ 2 1 4 は、取得したセッ ション鍵 K s 2 c をバス B S 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵 K s 1 b によって、バス B S 3 から取得したセッ ション鍵 K s 2 c を暗号化し、E (K s 1 b , K s 2 c) 生成する (ステップ S 1 1 9)。そして、暗号処理部 2 2 4 は、生成した E (K s 1 b , K s 2 c) を

バスBS3に出力する。バスBS3に出力されたE (Ks1b, Ks2c)は、コントローラ214により受理され、コントローラ214は、ステップS118において取得したデータとともに1つのデータ列LID//E (Ks1b, Ks2c) // ST1// ST2を生成し、ハッシュ関数を用いてハッシュ値H (LID//E (Ks1b, Ks2c) // ST1// ST2)を生成する（ステップS120）。そして、コントローラ214は、ハッシュ値H (LID//E (Ks1b, Ks2c) // ST1// ST2)をバスBS3を介して暗号処理部224へ出力する。

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したハッシュ値H (LID//E (Ks1b, Ks2c) // ST1// ST2)を暗号化し、E (Ks1b, H (LID//E (Ks1b, Ks2c) // ST1// ST2))生成する（ステップS121）。そして、暗号処理部224は、生成したE (Ks1b, H (LID//E (Ks1b, Ks2c) // ST1// ST2))をバスBS3に出力する。ここで、データ列LID//E (Ks1b, Ks2c) // ST1// ST2を受信ログと称し、E (Ks1b, H (LID//E (Ks1b, Ks2c) // ST1// ST2))は、受信ログに対してセッション鍵Ks1bを用いて電子署名を行なった署名データである。また、ログメモリ253に格納されていたセッション鍵Ks2cをセッション鍵Ks1bを用いて暗号化するのは、セッション鍵Ks2cの漏洩によるライセンスの流出の危険性を排除するためである。

コントローラ214は、バスBS3から署名データを受理すると、ステップS118において取得した受信ログを用いて、署名付き受信ログLID//E (Ks1b, Ks2c) // ST1// ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c) // ST1// ST2))を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS122）。

端末装置10は、署名付き受信ログLID//E (Ks1b, Ks2c) // ST1// ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c) // ST1// ST2))

// ST 1 // ST 2) ) を HD 20 から受理すると (ステップ S 123) 、受  
理したデータをネットワーク 30 を介してライセンス提供装置 40 へ出力する  
(ステップ S 124) 。そして、ライセンス提供装置 40 は、ネットワーク 30  
を介して署名付き受信ログ L ID//E (Ks1b, Ks2c) //ST1//  
5 ST2//E (Ks1b, H (L ID//E (Ks1b, Ks2c) //ST1//  
//ST2) ) を受信する。 (ステップ S 125)

図 14 を参照して、ライセンス提供装置 40 は、受信した署名付き受信ログ L  
ID//E (Ks1b, Ks2c) //ST1//ST2//E (Ks1b, H  
(L ID//E (Ks1b, Ks2c) //ST1//ST2) ) の検証を行な  
10 う (ステップ S 126) 。検証処理は次のように行なわれる。

配信制御部 412 は、署名付き受信ログを受理すると、まず、受理した署名付  
き受信ログの後半部である署名データ E (Ks1b, H (L ID//E (Ks1  
b, Ks2c) //ST1//ST2) ) を復号処理部 422 へ出力するととも  
15 に、セッション鍵発生部 414 にセッション鍵 Ks1b を発生するように指示す  
る。そして、復号処理部 422 は、セッション鍵 Ks1b によって署名データ E  
(Ks1b, H (L ID//E (Ks1b, Ks2c) //ST1//ST2) ) を復号し、HD 20 にて演算したハッシュ値を抽出する。一方、配信制御  
部 412 は、署名付き受信ログの前半部である受信ログ L ID//E (Ks1b,  
Ks2c) //ST1//ST2 のハッシュ値を演算し、復号処理部 422 によ  
20 り復号された HD 20 で演算されたハッシュ値と比較する。配信制御部 412 は、  
2 つのハッシュ値が一致したと判断すると、HD 20 から受理したデータ列は、  
正当なデータを含むものとしてライセンス提供装置 40 において承認される。

ステップ S 126 において HD 20 から受理した署名付き受信ログが承認され  
ると、配信制御部 412 は、受理したライセンス ID (L ID) に基づいてログ  
25 DB 404 を検索する (ステップ S 127) 。配信制御部 412 は、受理したラ  
イセンス ID (L ID) がログ DB 404 内に格納されており、HD 20 に対して確  
かに提供を行なったライセンスであると判断すると、受理したステータス S  
T 1, ST 2 の内容を確認する (ステップ S 128) 。

配信制御部 412 は、ステータス ST 1 が “受信待” であり、ステータス ST

2が”データ無”であるとき、HD 20に送信したはずのライセンスLICが何らかの異常によりHD 20において受理されていないと判断し、受信したデータ列に含まれる暗号化データE (Ks1b, Ks2c) を復号処理部422へ出力してセッション鍵Ks1bによってセッション鍵Ks2cを復号する。そして、  
5 復号されたセッション鍵Ks2cは、バスBS1を介して配信制御部412へ出力され、配信制御部412においてセッション鍵Ks2cが受理される（ステップS129）。

そして、配信制御部412は、異常発生時のセッション鍵Ks2aを今回受理したセッション鍵Ks2cと比較チェックする（ステップS130）。配信制御部412は、セッション鍵Ks2aとセッション鍵Ks2cとが一致していると判断すると、ライセンスLICの再書きに対する許可通知を端末装置10へ出力する（ステップS133）。

一方、ステップS126においてHD 20から受理したデータ列が承認されなかつたとき、ステップS127においてHD 20から受理したライセンスID (LID) がログDB404内に格納されておらず、HD 20に対して提供を行なったライセンスであると判断できないとき、ステップS128において、HD 20においてライセンスLICが受理されたものと判断されたとき、またはステップS130において、セッション鍵Ks2aがセッション鍵Ks2cと一致しないと判断されたときは、配信制御部412は、ライセンスの再送信は不可と判断し、バスBS1および通信装置450を介してエラー通知を端末装置10へ向けて出力し（ステップS131）、端末装置10は、ネットワーク30を介してエラー通知を受理すると（ステップS132）、処理が終了する。すなわち、ライセンス提供装置40において、ライセンスの再書きが拒否されて処理が終了する。

25 端末装置10のコントローラ108は、ステップS133においてライセンス提供装置40が output した許可通知を受理すると（ステップS134）、HD 20に対するセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD 20へ出力する（ステップS135）。

HD 20は、ライセンス提供装置40からの再書き処理許可通知に基づいて、

端末装置 10 からセッション鍵の生成要求通知を受理すると、新たにセッション鍵 Ks2b を生成し（ステップ S136）、ログメモリ 253 のバンク n のログに記録されているセッション鍵 Ks2c (=Ks2a) を、生成したセッション鍵 Ks2b に、ログのステータス ST1 を”受信待” に変更する（ステップ S137）。

以下、ステップ S138 からの一連の処理は、図 9 および図 10 において説明したステップ S21 から処理終了までの一連の処理において、セッション Ks2a に代えて新たに生成してセッション鍵 Ks2b が使用される他は、同様の処理が行なわれる。したがって、ステップ S138 からの一連の処理の説明は繰返し 10 になるので省略する。

なお、図 13～図 15 のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップ S101～S131、ステップ S133 およびステップ S142～S160 のいずれかのステップにおいて処理が中断した場合には、再び図 13～図 15 のフローチャートに従って再書込処理を行なうことができる。一方、ステップ S134～S141 のいずれかのステップにおいて処理が中断した場合には、図 9 および図 10 のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

このようにして、端末装置 10 に装着された HD20 が正規のクラス証明書 Cm1 を保持する機器であることを確認したうえで、クラス証明書 Cm1 に含まれて送信されたクラス公開鍵 KpCm1 によってライセンス提供装置 40 および HD20 でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置である HD20 における署名付き受信ログをライセンス提供装置 40 へ送信することで、

ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

[複製・移動]

図17は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図17を参照して、端末装置10にデータ記憶装置として2台のHD20, 21が装着可能であり、端末装置10を介してHD20からHD21へライセンスの複製または移動が行なわれる。

ここで、HD21は、HD20と異なるデータ記憶装置であるため、HD20とは異なる個別公開鍵K<sub>P</sub>o<sub>m</sub>5と個別秘密鍵K<sub>o</sub>m<sub>5</sub>とを保持している。この場合、HD21における識別子zは、HD20のz=2とは異なるz=5となる。また、HD21のクラスは、HD20のクラスと同じy=1として以下説明する。すなわち、HD20、HD21とも、クラス証明書C<sub>m</sub>1=K<sub>P</sub>c<sub>m</sub>1//I<sub>c</sub><sub>m</sub>1//E (K<sub>a</sub>, K<sub>P</sub>c<sub>m</sub>1//I<sub>c</sub><sub>m</sub>1) およびクラス秘密鍵K<sub>c</sub>m<sub>1</sub>を保持する。しかしながら、HD21のクラスがHD20のクラスと異なる(y≠1)場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、HD20とは異なったものとなる。

図18および図19は、図17に示すライセンスの複製・移動が可能なシステムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置10を介して端末装置10に装着されたHD20からHD21へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための第1および第2のフローチャートである。

図18を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置10のコントローラ108は、バスB<sub>S</sub>2およびHDインターフェース部110を介してHD21へクラス証明書の出力要求を出力する（ステップS201）。HD21においては、端子210およびATAインターフェース部212を介してクラス証明書の出力要求が受理されると（ステップS202）、コントローラ214は、認証データ保持部202からクラス証明書C<sub>m</sub>1=K<sub>P</sub>c<sub>m</sub>1//I<sub>c</sub><sub>m</sub>1//E

(K<sub>a</sub>, H (K<sub>P cm1</sub> // I<sub>cm1</sub>)) を読み出し、クラス証明書C<sub>m1</sub>をA T Aインターフェース部212および端子210を介して端末装置10へ出力する(ステップS203)。

5 端末装置10は、HD21からクラス証明書C<sub>m1</sub>を受理すると(ステップS204)、受理したクラス証明書C<sub>m1</sub>をHD20へ送信する(ステップS205)。

10 HD20では、端末装置10からHD21のクラス証明書C<sub>m1</sub>を受理すると(ステップS206)、認証部220およびコントローラ214によって受理したHD21のクラス証明書C<sub>m1</sub>が正当なクラス証明書であるか否かを認証する(ステップS207)。認証処理は、ライセンス提供装置40における認証処理(図9のステップS7)と同一であるため詳細な説明は省略する。

15 ステップS207において、コントローラ214は、正当なHD21のクラス証明書でないと判定した場合には、HD21のクラス証明書C<sub>m1</sub>を非承認として受理せず、エラー通知を端末装置10へ出力する(図19のステップS252)。そして、端末装置10においてエラー通知が受理されると(図15のステップS253)、配信セッションが終了する。

20 ステップS207において、HD21のクラス証明書C<sub>m1</sub>が正当な証明書であると判断されると、HD20のコントローラ214は、HD21のクラス証明書C<sub>m1</sub>を承認し、セッション鍵K<sub>s1a</sub>を生成するようにセッション鍵発生部226を制御し、セッション鍵発生部226は、セッション鍵K<sub>s1a</sub>を生成する(ステップS209)。

セッション鍵K<sub>s1a</sub>は、認証部220によって得られたHD21のクラス公開鍵K<sub>P cm1</sub>によって、暗号処理部222において暗号化され、暗号化データE (K<sub>P cm1</sub>, K<sub>s1a</sub>) が生成される(ステップS210)。

25 そして、コントローラ214は、暗号化データE (K<sub>P cm1</sub>, K<sub>s1a</sub>) を、A T Aインターフェース部212および端子210を介して端末装置10へ出力する(ステップS211)。

端末装置10は、暗号化データE (K<sub>P cm1</sub>, K<sub>s1a</sub>) を受理すると(ステップS212)、受理した暗号化データE (K<sub>P cm1</sub>, K<sub>s1a</sub>) をHD2

1 へ出力する（ステップS 213）。ここで、ライセンスID（LID）は、事前に管理ファイルを参照することで端末装置10が取得している。管理ファイルは、HD20に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部270に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

そして、HD21においては、コントローラ214が、端子210およびATAインターフェース部212を介してLID//E（K P c m 1, K s 1 a）を受理する（ステップS 214）。続いて、コントローラ214は、バスBS3を介してE（K P c m 1, K s 1 a）を復号処理部230へ与え、復号処理部230は、K c m保持部204に保持されるHD21に固有なクラス秘密鍵K c m 1によって復号処理することにより、セッション鍵K s 1 aを復号し、セッション鍵K s 1 aを受理する（ステップS 215）。

HD21のコントローラ214は、HD20で生成されたセッション鍵K s 1 aの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10は、HD21においてセッション鍵K s 1 aが受理された旨の通知を受理すると、セッション鍵の生成の要求通知をHD21へ出力する（ステップS 216）。HD21のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵K s 2 aを生成する（ステップS 217）。

セッション鍵発生部226は、セッション鍵K s 2 aを生成すると、バスBS3を介してコントローラ214へ出力し、コントローラ214は、セッション鍵K s 2 aを受ける。そして、コントローラ214は、最も古いログを格納したバンクを検索し、そこに処理中のセッションに対するログを新たに格納する（ステップS 218）。ステップS 218の詳細な動作は、図11および図12に示すフローチャートに従って行なわれる。ただし、HD21における処理と、HD20における同様の処理結果を区別するために最も古いログを格納したバンクは、

バンク n a であるとする。すなわち、図 1.1 および図 1.2 に示すフローチャートにおける変数 n を変数 n a と読み替えればよい。

したがって、ログメモリ 253 のバンク n a に、バンク n a - 1 に格納されるログの管理番号に 1 を加えた新しい管理番号と、ステップ S 214 において受理 5 したライセンス ID (LID) とセッション鍵 Ks2a とを格納し、ステータス ST1 を”受信待” にする。

続いて、HD21においては、続いて、暗号処理部 224 は、切換スイッチ 260 の接点 Pb を介して復号処理部 230 より与えられるセッション鍵 Ks1a によって、切換スイッチ 262 の接点 Pd と Pf とを順に切換えることによって 10 与えられるセッション鍵 Ks2a と個別公開鍵 KPom5 とからなる 1 つのデータ列を暗号化し、E (Ks1a, Ks2a // KPom5) を生成する (ステップ S 219)。そして、暗号処理部 224 は、E (Ks1a, Ks2a // KPom5) をバス BS3 に出力する。バス BS3 に出力された暗号化データ E (Ks1a, Ks2a // KPom5) は、コントローラ 214 により受理され、コ 15 ントローラ 214 は、受理した暗号化データとライセンス ID (LID) とを 1 つのデータ列としたデータ LID // E (Ks1a, Ks2a // KPom5) をATAインターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S 220)。

そして、端末装置 10 は、データ LID // E (Ks1a, Ks2a // KPom5) をHD21 から受理すると (ステップ S 221)、受理したデータをHD20 へ出力する (ステップ S 222)。

HD20 では、端子 210 およびATAインターフェース部 110 を介してデータ LID // E (Ks1a, Ks2a // KPom5) を受理すると (ステップ S 223)、復号処理部 228 においてセッション鍵 Ks1a による復号処理を 25 実行し、HD21 で生成されたセッション鍵 Ks2a、およびHD21 の個別公開鍵 KPom5 を抽出して受理する (ステップ S 224)。そして、復号処理部 228 は、復号したセッション鍵 Ks2a をバス BS3 を介してコントローラ 214 へ出力し、コントローラ 214 は、セッション鍵 Ks2a を受ける。そして、コントローラ 214 は、最も古いログを格納したバンクに、処理中のセッション

に対するログを新たに格納する（ステップS 225）。ステップS 225の詳細な動作は、図20に示すフローチャートに従って行なわれる。図20を参照して、ステップS 225は、ログメモリ253の最新ログが記録されたバンクn-1を特定し、かつ、バンクn-1に格納された管理番号mを取得するステップS 225aと、バンクnに、管理番号m+1、ライセンスID（LID）、セッション鍵Ks2a、およびクラス公開鍵KPCmyを格納し、かつ、ステータス領域を“送信待”に設定するステップS 225bとから成る。そして、ステップS 225aの詳細な動作は、図12に示すフローチャートに従って行なわれる。したがって、コントローラ214は、図20および図12に示すフローチャートに従つて、ステップS 223において受理したライセンスID（LID）とステップS 224で受理したセッション鍵Ks2aとをバンクnに格納し、ステータスST1を“送信待”にする。

HD20では、ステップS 225の処理を終えると、HD20のコントローラ214は、その旨をATAインターフェース部212および端子210を介して端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20からの通知を受理すると、HD20のセキュアデータ記憶部250において、HD20からHD21へ送信するライセンスLICが格納されているLBA（格納LBA）をバスBS2およびHDインターフェース110を介してHD20へ出力する（ステップS 226）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介して送信対象のライセンスLICの格納LBAを受理すると（ステップS 227）、その受理した格納LBAをセキュアデータ記憶部250のログメモリ253のバンクnに記憶する（ステップS 228）。

そして、コントローラ214は、受理した格納LBAに格納されるライセンスLICに対応する有効フラグ領域252のフラグが“有効”であるか“無効”であるかを確認する（ステップS 229）。コントローラ214は、有効フラグが“有効”であると、格納LBAに格納されているライセンスLICを取得する（ステップS 230）。

図19を参照して、HD20では、コントローラ214が、対象のライセンス

L I Cを取得すると、ライセンスL I Cに含まれるライセンスI D (L I D)と、  
ステップS 2 2 3において受理し、ログメモリ2 5 3のバンクn aに格納されて  
いるログに記憶されているライセンスI D (L I D)とを比較し、一致している  
か否かをチェックする (ステップS 2 3 1)。コントローラ2 1 4は、一致して  
5 いると判断すると、取得したライセンスL I Cに含まれる制御情報A Cを確認し  
て利用制限がかけられていないかをチェックする (ステップS 2 3 2)。

コントローラ2 1 4は、制御情報A CにおいてライセンスL I Cの利用が禁止  
されていないことを確認すると、取得したライセンスL I Cを暗号処理部2 3 2  
に与える。暗号処理部2 3 2は、復号処理部2 2 8によって得られたH D 2 1の  
10 個別公開鍵K P o m 5によってライセンスL I Cを暗号化して暗号化データE  
(K P o m 5, L I C)を生成する (ステップS 2 3 3)。そして、暗号処理部  
2 3 2は、暗号化データE (K P o m 5, L I C)を切替スイッチP cを介して  
暗号処理部2 2 4へ出力し、暗号処理部2 2 4は、暗号処理部2 3 2から受けた  
15 暗号化データを復号処理部2 2 8から受けたセッション鍵K s 2 aによって暗号  
化し、暗号化データE (K s 2 a, E (K P o m 5, L I C))を生成する (ス  
テップS 2 3 4)。

続いて、コントローラ2 1 4は、対象のライセンスL I Cに含まれる制御情報  
A Cに基づいて、H D 2 0からH D 2 1へのライセンスL I Cの送信が「移動」  
であるか「複製」であるかを確認する (ステップS 2 3 5)。コントローラ2 1  
20 4は、「移動」であると確認したときは、その対象のライセンスL I Cに対応す  
る、すなわち、格納L B Aに対応する有効フラグ領域2 5 2のフラグを“無効”  
に変更する (ステップS 2 3 6)。一方、コントローラ2 1 4は、「複製」であ  
ると確認したときには、当該ライセンスL I CがH D 2 0に残っていてよいの  
で、有効フラグ領域2 5 2のフラグの変更は行なわずに次の処理 (ステップS 2  
25 3 7)へ移行する。

コントローラ2 1 4は、有効フラグ領域2 5 2の処理が終わると、ログメモリ  
2 5 3のバンクnに格納されているログのステータスS T 1を“送信済”に変更  
し (ステップS 2 3 7)、A T Aインターフェース部2 1 2および端子2 1 0を  
介して暗号化データE (K s 2 a, E (K P o m 5, L I C))を端末装置1 0

へ送信する（ステップS238）。

一方、ステップS229において受理した格納LBAに対応する有効フラグ領域252のフラグが“無効”であったとき、ステップS231においてライセンスID（LID）が一致しないとき、または、ステップS232において、取得5したライセンスLICに含まれる制御情報ACにより当該ライセンスLICの利用が禁止されているときは、コントローラ214は、端末装置10に対してエラー通知を出力し（ステップS252）、端末装置10においてエラー通知が受理されると（ステップS253）、処理が終了する。

端末装置10は、ステップS238においてHD20から出力された暗号化データE（Ks2a, E（Kpom5, LIC））を受理すると（ステップS239）、受理した暗号化データをHD21へ出力する（ステップS240）。

HD21では、コントローラ214が、端子210およびATAインターフェース部212を介して暗号化データE（Ks2a, E（Kpom5, LIC））を受理し（ステップS241）、バスBS3へ出力する。復号処理部228は、15セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE（Ks2a, E（Kpom5, LIC））を復号し、HD21において、ライセンスLICが個別公開鍵Kpom5により暗号化された暗号化ライセンスE（Kpom5, LIC）が受理される（ステップS242）。そして、復号処理部228は、暗号化ライセンスE（Kpom5, LIC）をバスBS3へ出力する。20

コントローラ214の指示によって、暗号化ライセンスE（Kpom5, LIC）は、復号処理部216において個別秘密鍵Kom5によって復号され、HD21においてライセンスLICが受理される（ステップS243）。

コントローラ214は、ライセンスLICの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。25端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD21においてライセンスLICが受理された旨の通知を受理すると、HD21のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBA（格納LBA）をバスBS2およびHDインターフェース部212へ送信する（ステップS244）。

5 一フェース 110 を介して HD 21 へ出力する (ステップ S 244)。HD 21 のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介してライセンス L I C を格納する格納 L B A を受理すると (ステップ S 245)、その受理した格納 L B A をログメモリ 253 のバンク n に格納されるログの L B A 領域 2544 に記録する (ステップ S 246)。

10 そして、コントローラ 214 は、受理したライセンス L I C に含まれるライセンス I D (L I D) と、ステップ S 214 において受理したライセンス L I D (L I D) とを比較し、一致しているか否かをチェックする (ステップ S 247)。コントローラ 214 は、L I D が一致しており、受理したライセンス L I C が正しいものであると判断すると、端末装置 10 から受理したセキュアデータ記憶部 250 内の格納 L B A に対応する領域に、受理したライセンス L I C を記憶する (ステップ S 248)。

15 コントローラ 214 は、指定された格納 L B A にライセンス L I C を記憶すると、有効フラグ領域 252 のその格納 L B A に対応するフラグを“有効”にする (ステップ S 249)。そして、コントローラ 214 は、さらに、ログメモリ 253 のバンク n に格納されたログのステータス S T 1 を“受信済”にし (ステップ S 250)、複製・移動セッションにおける一連の処理が終了したことを ATA インターフェース部 212 および端子 210 を介して端末装置 10 に通知する。

20 そして、端末装置 10 において、HD 21 からの処理終了通知が受理されると、HD 20 から HD 21 へのライセンス L I C の複製・移動セッションが正常終了する。

25 一方、ステップ S 247 において、HD 20 のコントローラ 214 が、L I D が一致しておらず、受理したライセンス L I C が正しくないと判断すると、ATA インターフェース部 212 および端子 210 を介してエラー通知を端末装置 10 へ出力し (ステップ S 251)、端末装置 10 においてエラー通知が受理されると (ステップ S 253)、HD 20 から HD 21 へのライセンス L I C の複製・移動セッションが異常終了する。

ここで、配信セッションのときと同様に、図 18 および図 19 に示された複製・移動セッションにおける一連の処理において、ステップ S 227 からステッ

PS 252 の処理中に異常が発生し、処理が中断したときは、再書き込み処理の対象となる。

ここで、図18および図19に示された複製・移動セッションにおいて、ステップS227からステップS235までの処理を再書き込み処理の対象としたのは、  
5 この一連の処理がHD20の内部処理であり、ステップS226の終了後は、ステップS238まで端末装置10においていずれのステップを処理中に処理が中断したかを特定できないため、すべてステップS236が実行されてライセンスが無効化されたものとし、必ず再書き込み処理の対象としたものである。

そして、ステップS236からステップS247までの処理を再書き込み処理の対象としたのは、「移動」の場合、この間は、HD20内のライセンスがステップS236において無効化され、かつ、HD21内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。

また、ステップS248からステップS250までの処理を再書き込み処理の対象としたのは、ステップS249、S250については、これらの処理はステップS248におけるライセンス書き込み後の処理であるから本来は処理が終了しているところ、端末装置10からはステップS248の終了が特定できないため、ステップS248が終了していないものとみなして、ステップS248からステップS250を再書き込み処理の対象としたものである。なお、ステップS248が終了していて再書き込み処理が行なわれた場合には、再書き込みは拒否される。  
15

また、ステップS251の処理を再書き込み処理の対象としたのは、本来、この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置10においては、ステップS251において処理が中断したことを特定することができないため、再書き込み処理の対象としたものである。

25 なお、端末装置10において、上述したように当該セッションがライセンスの「複製」であると判断できる場合、あるいはステップS227からステップS235およびステップS249からステップS251のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書き込み処理とする必要はなく、図18および図19に示された複製・移動セッションを再度実行すればよい。

## [移動／複製における再書き込み]

図21～図23は、図18および図19において示した複製・移動セッションの処理フローにおけるステップS227からステップS252の処理中に異常が発生したときに行なわれる再書き込み処理の第1から第3のフローチャートである。

5 図21を参照して、端末装置10は、ステップS227からステップS252の処理中に異常が発生したと判断すると、ライセンスID(LID)とライセンスLICの再送要求とをデータ列LID//再送要求としてHD20へ出力する(ステップS301)。HD20では、コントローラ214が、端子210およびATAインターフェース部212を介してLID//再送要求を受理する(ステップS301a)。そして、ログの複製処理を行なう(301b)。複製処理では、ログメモリ253内にステップS301aにおいて受理したLIDを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ253の最も古いログを格納しているバンクnに、検索されたLIDを含むログを複製し、変数ERR="偽"とする。一方、ログメモリ253内にステップS301aにおいて受理したLIDを含むログが格納されていない場合には、変数ERR="真"とする。この複製処理の詳細な動作は、図16に示すフローチャートに従って行なわれる。

10

15

そして、コントローラ214は、ステップS301aの処理結果の判定、すなわち、変数ERRが"真"、"偽"のいずれであるかを判定する(ステップS301b)。"真"の場合、受理したLIDを含むログがバンクnへ複製されたことを示すので、再送要求に対する処理を開始するために次のステップS302へ移行する。"偽"の場合、受理したLIDを含むログがログメモリ253に格納されていなかった、つまり、HD20において受理したLIDによって特定されるライセンスLICの入出力処理がなされていなかったことを示すので、再送要求に対応不能と判断し、図23のステップS372へ移行し、エラー通知を端末装置10に対して出力する。端末装置10においてはエラー通知が受理されると(ステップS373)、処理が終了する。

20

25

HD20において、ステップS301bにおいて変数ERR="偽"を確認すると、コントローラ214は、ログメモリ253のバンクnに複製され、かつ、

格納されているログのステータスST1の状態を確認する（ステップS302）。コントローラ214は、ステータスST1が“送信待”または“送信済”でないとき、すなわち複製・移動セッションにおいてライセンスLICの送信側でないときは、図23に示すステップS371へ処理が移行する。

5 HD20のコントローラ214は、ステータスST1が“送信待”または“送信済”であるときは、セッション鍵発生部226にセッション鍵を生成するよう10に指示し、セッション鍵発生部226は、セッション鍵Ks1aを生成する（ステップS303）。セッション鍵Ks1bが生成されると、コントローラ214は、中断以前に受理した、ライセンスLICの移動／複製先のHD21のクラス15公開鍵KPCM1を、ログメモリ253のバンクnに格納されたログから取得する（ステップS304）。ここで、移動／複製先のHD21から再びクラス証明書Imc1を受理することなくログに記憶されるクラス公開鍵KPCM1を用いるのは、再書き込み処理におけるなりすまし攻撃によるライセンスLICの漏洩を防ぐためである。したがって、再び、クラス証明書Imc1を受理する場合には、HD20において、中断した処理において受理したクラス証明書と再書き込み処理において受理したクラス証明書とが同一か否かを確認する必要がある。たとえば、再書き込み処理において受理したクラス証明書Imc1に含まれるクラス公開鍵とログに記録されるクラス公開鍵を比較して再書き込み処理を行なうか否かを判断する。

そして、HD21では、そのクラス公開鍵KPCM1によって、セッション鍵20Ks1bが暗号処理部222によって暗号化され、暗号化データE（KPCM1, Ks1b）が生成される（ステップS305）。コントローラ214は、生成された暗号化データE（KPCM1, Ks1b）とライセンスID（LID）とをデータ列LID//E（KPCM1, Ks1b）としてATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS306）。

端末装置10は、LID//E（KPCM1, Ks1b）を受理すると（ステップS307）、受理したLID//E（KPCM1, Ks1b）をHD21へ出力する（ステップS308）。

HD21において、コントローラ214は、端子210およびATAインター

フェース部212を介してLID//E (KPCM1, Ks1b) を受理すると (ステップS309) 、バスBS3を介してE (KPCM1, Ks1b) を復号処理部230へ与える。そうすると、復号処理部230は、Kcm保持部204に保持されるHD21に固有なクラス秘密鍵Kcm1によって復号処理を実行してセッション鍵Ks1bを復号し、セッション鍵Ks1bを受理する (ステップS310) 。

HD21のコントローラ214は、HD20で生成されたセッション鍵Ks1bの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介してHD21からの通知を受理すると、HD21のログメモリ253に格納されるログのHD20への出力要求をバスBS2およびHDインターフェース部110を介してHD21へ出力する (ステップS311) 。HD21のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理する (ステップS312) 。そして、HD20におけるステップS301aと同様にログの複製処理を行なう (ステップS213a) 。複製処理時、ログメモリ253内にステップS309において受理したLIDを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ253の最も古いログを格納しているバンクn aに、検索されたLIDを含むログを複製し、変数ERRa = “偽”とする。一方、ログメモリ253内にステップS309において受理したLIDを含むログが格納されていない場合には、ERRa = “真”とする。このステップS312aの詳細な動作は、図16に示すフローチャートに従って行なわれる。ただし、HD21における処理と、HD20における同様の処理結果を区別するために変数nを変数naとし、変数ERRを変数ERRaとする。すなわち、図16のステップS112bに相当する図12に示すフローチャートにおける変数nを変数naに、変数ERRを変数ERRaにそれぞれ読み替えればよい。

そして、コントローラ214は、ステップS312aの処理結果の判定、すなわち、ERRaが“真”、“偽”的いずれであるかを判定する (ステップS3212b) 。“偽”的場合、受理したLIDを含むログがバンクnaへ複製された

ことを示すので、再送要求に対する処理を開始するために次のステップ S 313 へ移行する。“真”の場合、受理した L I D を含むログがログメモリ 253 に格納されていなかった、つまり、HD 21において、ステップ S 313において受理した L I D によって特定されるライセンス L I C の入出力処理がなされなかつたことを示すので、再送要求に対応不能と判断し、図 23 のステップ S 371 へ移行し、エラー通知を端末装置 10 に対して出力する。端末装置 10 においては、エラー通知が受理されると（ステップ S 373）、処理が終了する。

HD 21において、ステップ S 312bにおいて E R R a = “偽”を確認すると、コントローラ 214 は、ログメモリ 253 のバンク n a に格納されているログの格納 L B A に対する領域に記憶されるライセンス L I C のライセンス I D (L I D) と、ログメモリ 253 のバンク n a に格納されているログのライセンス I D (L I D) とが一致するか否かを確認する（ステップ S 313）。

コントローラ 214 は、ライセンス I D (L I D) が一致すると、さらに、ログメモリ 253 のバンク n a に格納されているログの格納 L B A に対応する有効フラグ領域 252 のフラグを確認し、そのライセンス L I C が有効であるか無効であるかを確認する（ステップ S 314）。コントローラ 214 は、有効フラグ領域 252 のフラグが“有効”であるときは、ログメモリ 253 のバンク n a に格納されているログのステータス S T 2 を“データ有”に変更し（ステップ S 315）、次の処理（ステップ S 318）へ移行する。一方、コントローラ 214 は、有効フラグ領域 252 のフラグが“無効”であるときは、ログメモリ 253 のバンク n a に格納されているログのステータス S T 2 を“移動済”に変更し（ステップ S 316）、次の処理（ステップ S 318）へ移行する。

また、コントローラ 214 は、ステップ S 313において両ライセンス I D (L I D) が一致しないときは、ログメモリ 253 のバンク n a に格納されているログのステータス S T 2 を“データ無”に変更する（ステップ S 317）。

ステータス S T 2 の変更処理がなされると、コントローラ 214 は、ログメモリ 253 のバンク n a からライセンス I D (L I D)、ステータス S T 1、S T 2、セッション鍵 K s 2c および格納 L B A を取得する（ステップ S 318）。ここで、この処理は、図 9 および図 10 のフローチャートに従った配信セッショ

ンの中断に対する処理であるため、HD 2 1 のログメモリ 2 5 3 に格納されている当該処理のログに記憶されているセッション鍵はK s 2 a であるが、説明の関係上、ログメモリ 2 5 3 のバンク n から取得したセッション鍵をK s 2 c としている。そして、コントローラ 2 1 4 は、取得したセッション鍵K s 2 c をバス B 5 S 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵K s 1 b によってセッション鍵K s 2 c を暗号化し、E (K s 1 b, K s 2 c) 生成する (ステップ S 3 1 9)。そして、暗号処理部 2 2 4 は、生成したE (K s 1 b, K s 2 c) をバス B S 3 に出力する。バス B S 3 に出力されたE (K s 1 b, K s 2 c) は、コントローラ 2 1 4 により 10 受理され、コントローラ 2 1 4 は、ステップ S 3 1 8 において取得したデータとともに 1 つの受信ログ L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2 を生成し、そのハッシュ値 H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 15 2) を生成する (ステップ S 3 2 0)。そして、コントローラ 2 1 4 は、ハッシュ値 H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2) をバス B S 3 を介して暗号処理部 2 2 4 へ出力する。

暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵K s 1 b によって、バス B S 3 から取得したハッシュ値 H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2) を暗号化し、署名データ E (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) 生成する (ステップ S 3 2 1)。そして、暗号処理部 2 2 4 は、生成したE (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) をバス B S 3 に出力する。

コントローラ 2 1 4 は、バス B S 3 から署名データを取得すると、ステップ S 25 3 1 8 において取得した受信ログを用いて、署名付き受信ログ L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2 // E (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) を生成し、署名付き受信ログ L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2 // E (K s 1 b, H (L I D // E (K s 1 b, K s 2 c) // S T 1 // S T 2)) と格納 L B

Aとを、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS322）。

図22を参照して、端末装置10は、署名付き受信ログLID//E (Ks1b, Ks2c) //ST1//ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))と格納LBAとをHD21から受理すると（ステップS323）、受理したデータをHD20へ出力する（ステップS324）。

HD20において、コントローラ214は、署名付き受信ログLID//E (Ks1b, Ks2c) //ST1//ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))を受理すると（ステップS325）、受理した署名付き受信ログの検証を行なう（ステップS326）。検証処理は、以下のように行われる。

HD20のコントローラ214は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データE (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))を復号処理部228へ出力するとともに、セッション鍵発生部226にセッション鍵Ks1bを発生するように指示する。そして、復号処理部228は、セッション鍵Ks1bによって署名データE (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))を復号し、HD21によって求められたハッシュ値を抽出する。一方、HD20のコントローラ214は、署名付き受信ログの前半部である受信ログLID//E (Ks1b, Ks2c) //ST1//ST2のハッシュ値を演算し、復号処理部228により抽出されたハッシュ値と比較する。HD20のコントローラ214は、2つのハッシュ値が一致したと判断すると、HD21から受理した受信ログは、正当なデータを含むものとしてHD20において承認される。

ステップS326において承認されると、HD20のコントローラ214は、ステップS325において承認した受信ログに含まれるライセンスID (LID) をログメモリ253のバンクnに格納されるライセンスID (LID) と比較する（ステップS327）。

コントローラ 214 は、ライセンス ID (LID) が一致すると、受信ログに含まれる暗号データ E (Ks1b, Ks2c) を復号処理部 228 へ出力し、復号処理部 228 は、セッション鍵発生部 226 から受けるセッション鍵 Ks1b によってセッション鍵 Ks2c を復号し、セッション鍵 Ks2c が受理される  
5 (ステップ S328)。そして、復号されたセッション鍵 Ks2c は、バス BS 3 を介してコントローラ 214 へ出力される。続いて、コントローラ 214 は、エラー発生時のセッション鍵、すなわち、バンク n のログに記録されているセッション鍵 Ks2a と、今回、承認した受信ログに含まれていたセッション鍵 Ks2c とを比較する (ステップ S329)。コントローラ 214 は、セッション鍵 Ks2a とセッション鍵 Ks2c とが一致していると判断すると、受理したステータス ST1, ST2 の内容を確認する (ステップ S330)。

HD20 のコントローラ 214 は、受信した受信ログのステータス ST1 が “受信待” であり、受信ログのステータス ST2 が “データ無” であるとき、HD21 に送信したはずのライセンス LIC が何らかの異常により HD21 において受理されていないと判断する。そうすると、HD20 のコントローラ 214 は、さらに、ログメモリ 253 のバンク n のログの格納 LBA に記憶されるライセンス LIC のライセンス ID (LID) と、ログメモリ 253 のバンク n のログのライセンス ID (LID) とが一致するか否かを確認する (ステップ S331)。HD20 のコントローラ 214 は、ライセンス ID (LID) が一致すると、さらに、ログメモリ 253 のバンク n のログの格納 LBA に対応する有効フラグ領域 252 のフラグを確認し、そのライセンス LIC が有効であるか無効であるかを確認する (ステップ S332)。そして、コントローラ 214 は、有効フラグ領域 252 のフラグが “無効” であるときは、その有効フラグ領域 252 のフラグを “有効” に変更する (ステップ S333)。一方、コントローラ 214 は、有効フラグ領域 252 のフラグが “有効” であるときは、次の処理 (ステップ S334) へ移行する。そして、コントローラ 214 は、ログメモリ 253 のバンク n のログの格納 LBA と許可通知とを ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S334)。

端末装置 10 のコントローラ 108 は、HD20 から HD インターフェース部

110 およびバスB S 2 を介して対象のライセンスL I Cが格納される格納L B Aと許可通知とを受理すると（ステップS 3 3 5）、HD 2 1 に対してセッション鍵の生成の要求通知をバスB S 2 およびHDインターフェース部1 1 0 を介してHD 2 1 へ出力する（ステップS 3 3 6）。

5 HD 2 1 は、端末装置1 0 からセッション鍵の生成要求通知を受理すると、新たにセッション鍵K s 2 b を生成し（ステップS 3 3 7）、ログメモリ2 5 3 のバンクn a のログに記憶されているセッション鍵K s 2 c （K s 2 a）を、生成したセッション鍵K s 2 b に、ログのステータスS T 1 を“受信待”に変更する（ステップS 3 3 8）。

10 以下、ステップS 3 3 9 からの一連の処理は、図1 8 および図1 9 において説明したステップS 2 1 9 から処理終了までの一連の処理において、セッション鍵K s 2 a に代えて新たに生成したセッション鍵K s 2 b が使用される他は、同様の処理が行なわれる。したがって、ステップS 3 3 9 に続く一連の処理の説明は繰返しになるので省略する。

15 なお、ステップS 3 3 5 において処理を終了し、HD 2 0 にライセンスを残すことも可能である。この場合、図1 8 および図1 9 に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

なお、図2 1 ～図2 3 のフローチャートに示されるライセンスの移動または複製における再書き込み処理の中断に対しては、ステップS 3 0 1 ～S 3 4 4 およびステップS 3 4 7 ～S 3 7 1 のいずれかのステップにおいて処理が中断した場合には、再び図2 1 ～図2 3 に示されるフローチャートに従って再書き込み処理を行なうことができる。一方、ステップS 3 2 5 ～S 3 4 6 のいずれかのステップにおいて処理が中断した場合には、図1 8 および図1 9 のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

25 このようにして、端末装置1 0 に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先のHD 2 1 から受取ったクラス証明書C m 1 が有効であることを確認し、クラス証明書C m 1 に含まれて送信されたクラス公開鍵K P c m 1 によってライセンスの複製・移動が行

なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンスの複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるHD 2 1における複製・移動セッションの対象となったライセンスL I Cに対する受信ログを送信側のデータ記憶装置であるHD 2 0へ送信し、HD 2 0において、自身のログメモリ2 5 3に格納されるログの内容と、そのログに記憶される格納L B Aによって特定されるセキュアデータ記憶部2 5 0の領域に記憶されるライセンスL I Cとを比較し、さらに有効フラグ領域2 5 2に記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、2つのデータ記憶装置HD 2 0およびHD 2 1に利用可能なライセンスが重複して存在することのない安全な再書き込み処理が提供される。

このように、本発明は、複製・移動セッションの中断によるライセンスL I Cの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処理手順を提供するとともに、再書き込み処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

なお、図18～図23におけるHD 2 1の処理ステップS 2 0 2, 2 0 3, S 2 1 4, S 2 1 5, S 2 1 7～S 2 2 0, S 2 4 1～S 2 4 3, S 2 4 5～S 2 5 1, S 3 0 9, S 3 1 0, S 3 1 2～S 3 2 2, S 3 3 7～S 3 4 0, S 3 6 1～S 3 6 3, S 3 6 5～S 3 7 1は、図9、図10および図13～図15におけるHD 2 0の処理ステップS 2, S 3, S 1 6, S 1 7, S 1 9～S 2 2, S 3 3～S 3 5, S 3 7～S 4 3, S 1 0 9, S 1 1 0, S 1 1 2～S 1 2 2, S 1 3 6～S 1 3 9, S 1 5 0～S 1 5 2, S 1 5 4～S 1 6 0とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるHD 2 1の処理とライ

センスの配信処理時におけるHD 20の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（HD 20, HD 21）においてライセンスを書込むためのデータ記憶装置における処理である。

#### [再生許諾]

5 再び図5を参照して、コンテンツデータを再生する再生回路150を備えた端末装置10にデータ記憶装置としてのHD 20が装着され、コンテンツデータの再生許諾は、HD 20から端末装置10内の再生回路150に対して行なわれる。

10 図24は、端末装置10のユーザが端末装置10から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置10に装着されたHD 20から端末装置10内の再生回路150へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

15 図24を参照して、端末装置10のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置10のコントローラ108は、バスBS2を介して再生回路150へクラス証明書の出力要求を出力する（ステップS401）。再生回路150において、認証データ保持部1502は、バスBS2からクラス証明書の出力要求を受けると（ステップS402）、保持しているクラス証明書Cp3=Kp3//Ic3//E (Ka, H (Kp3//Ic3))をバスBS2へ出力する（ステップS403）。

20 コントローラ108は、バスBS2からクラス証明書Cp3を受理すると（ステップS404）、受理したクラス証明書Cp3をバスBS2およびHDインターフェース部110を介してHD 20へ出力する（ステップS405）。

25 HD 20では、端末装置10からクラス証明書Cp3を受理すると（ステップS406）、受理したクラス証明書Cp3が正当なクラス証明書であるか否かを検証する（ステップS407）。検証処理は、複製・移動セッションにおけるステップS207において説明したのと同様の方法で行なわれ、説明は省略する。

ステップS407において、クラス証明書Cp3が正当な証明書であると判断された場合、コントローラ214は、クラス証明書Cp3を承認し、クラス証明書Cp3に含まれるクラス公開鍵Kp3を受理する（ステップS408）。そして、次の処理（ステップS409）へ移行する。コントローラ214は、正

当なクラス証明書でない場合には、クラス証明書C p 3を非承認とし、クラス証明書C p 3を受理せずにエラー通知を端末装置10へ出力し（ステップS 4 3 5）、端末装置10においてエラー通知が受理されると（ステップS 4 3 6）、再生許諾セッションが終了する。

5 ステップS 4 0 8においてクラス公開鍵K P c p 3が受理されると、HD 2 0 のセッション鍵発生部226は、セッション鍵K s 1 dを生成する（ステップS 4 0 9）。セッション鍵K s 1 dは、受理されたクラス公開鍵K P c p 3によつて、暗号処理部222において暗号化され、暗号化データE（K P c p 3, K s 1 d）が生成される（ステップS 4 1 0）。

10 そして、コントローラ214は、暗号処理部222からバスB S 3を介して暗号化データE（K P c p 3, K s 1 d）を受けると、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS 4 1 1）。

15 端末装置10において、HDインターフェース部110およびバスB S 2を介してコントローラ108が暗号データE（K P c p 3, K s 1 d）を受理すると（ステップS 4 1 2）、コントローラ108は、受理した暗号化データE（K P c p 3, K s 1 d）をバスB S 2を介して再生回路150へ出力する（ステップS 4 1 3）。再生回路150の復号処理部1506は、バスB S 2から暗号化データE（K P c p 3, K s 1 d）を受けると（ステップS 4 1 4）、K c p保持部1504に保持される再生回路150に固有なクラス秘密鍵K c p 3によつて復号処理することによりセッション鍵K s 1 dを復号し、セッション鍵K s 1 dが受理される（ステップS 4 1 5）。

20 セッション鍵K s 1 dが受理されると、セッション鍵発生部1508は、セッション鍵K s 2 dを生成し（ステップS 4 1 6）、生成したセッション鍵K s 2 dを暗号処理部1510に与える。暗号処理部1510は、復号処理部1506から受けるセッション鍵K s 1 dをセッション鍵K s 2 dにより暗号化し、暗号化データE（K s 1 d, K s 2 d）を生成する（ステップS 4 1 7）。そして、暗号処理部1510は、暗号化データE（K s 1 d, K s 2 d）をバスB S 2へ出力する（ステップS 4 1 8）。

25 コントローラ108は、バスB S 2から暗号化データE（K s 1 d, K s 2

d) を受理し (ステップS 4 1 9) 、受理したデータをバスB S 2 およびHDインターフェース部1 1 0を介してHD 2 0へ出力する (ステップS 4 2 0) 。

HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介して暗号化データE (K s 1 d, K s 2 d) を受理すると (ステップS 4 2 1) 、受理したデータをバスB S 3へ出力する。復号処理部2 2 8は、セッション鍵発生部2 2 6から与えられたセッション鍵K s 1 dを用いてバスB S 3に出力された暗号化データE (K s 1 d, K s 2 d) を復号し、HD 2 0においてセッション鍵K s 2 dが受理される (ステップS 4 2 2) 。そして、コントローラ2 1 4は、セッション鍵K s 2 dが受理されると、その旨の通知をATAインターフェース部2 1 2および端子2 1 0を介して端末装置1 0へ出力する。

端末装置1 0のコントローラ1 0 8は、HDインターフェース部1 1 0およびバスB S 2を介してHD 2 0においてセッション鍵K s 2 dが受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンスL I Cが格納されているセキュアデータ記憶部2 5 0のL B AをバスB S 2およびHDインターフェース部1 1 0を介してHD 2 0へ出力する。

HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介して対象のライセンスL I Cが格納されているL B Aを受理すると (ステップS 4 2 4) 、そのL B Aに格納されるライセンスL I Cに対応する有効フラグ領域2 5 2のフラグが“有効”であるか“無効”であるかを確認する (ステップS 4 2 5) 。

コントローラ2 1 4は、有効フラグ領域2 5 2のフラグが“有効”であると、受理したL B Aに基づいて、対象のライセンスL I Cをセキュアデータ記憶部2 5 0から取得する (ステップS 4 2 6) 。そして、コントローラ2 1 4は、取得したライセンスL I Cに含まれる制御情報A Cの内容を確認する (ステップS 4 2 7) 。コントローラ2 1 4は、制御情報A Cにおいて利用回数が指定されているときは、制御情報A Cの利用回数を1増分し、次の処理 (ステップS 4 2 9) へ移行する。一方、コントローラ2 1 4は、制御情報A Cにより再生制限がかけられていないときは、取得したライセンスL I Cに含まれるコンテンツ鍵K cをバスB S 3へ出力する。

暗号処理部 224 は、復号処理部 228 から受けるセッション鍵  $K_{s2d}$  によりバス BS3 上に出力されたコンテンツ鍵  $K_c$  を暗号化して暗号化データ  $E$  ( $K_{s2d}$ ,  $K_c$ ) を生成し (ステップ S429) 、生成したデータをバス BS3 へ出力する。そして、コントローラ 214 は、バス BS3 上に出力された暗号化データ  $E$  ( $K_{s2d}$ ,  $K_c$ ) を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S430)。

端末装置 10 のコントローラ 108 は、HD インターフェース部 110 およびバス BS2 を介して暗号化データ  $E$  ( $K_{s2d}$ ,  $K_c$ ) を受理すると (ステップ S431) 、受理したデータをバス BS2 へ出力する (ステップ S432)。

10 再生回路 150 の復号処理部 1512 は、バス BS2 から暗号化データ  $E$  ( $K_{s2d}$ ,  $K_c$ ) を受理すると (ステップ S433) 、セッション鍵発生部 1508 から与えられるセッション鍵  $K_{s2d}$  を用いて暗号化データ  $E$  ( $K_{s2d}$ ,  $K_c$ ) を復号する。これにより、再生回路 150 においてコンテンツ鍵  $K_c$  が受理され (ステップ S434) 、一連の再生許諾セッションの処理が正常終了する。

15 一方、ステップ S425 において、有効フラグ領域 252 のフラグが “無効” であったとき、またはステップ S427 において、制御情報 AC に含まれる内容が再生不可であったときは、コントローラ 214 は、端末装置 10 に対してエラー通知を出力し (ステップ S435) 、端末装置 10 においてエラー通知が受理されると (ステップ S436) 、再生許諾セッションが終了する。

20 このようにして、データ記憶装置である HD 20 から端末装置 10 に備えられる再生回路 150 への再生許諾に関しても、再生回路 150 が正規のクラス証明書 Cp3 を保持していること、およびクラス証明書 Cp3 に含まれて送信されたクラス公開鍵  $K_{PcP3}$  が有効であることを確認した上でコンテンツ鍵  $K_c$  が再生回路 150 へ送信され、不正なコンテンツデータの再生を禁止することができる。

25 なお、フローチャートにおいて図示しないが、再生回路 150 は、コンテンツの再生許諾がなされ、コンテンツ鍵  $K_c$  を受理すると、HD 20 から出力された暗号化コンテンツデータ  $E$  ( $K_c$ ,  $D_c$ ) を復号処理部 1514 において復号し、再生部 1516 において復号処理部により復号されたデータ  $D_c$  が再生され、D

A変換部1518によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子1520へ再生信号が出力される。

このように、HD20では、ライセンスの漏洩が無いように安全に保護し、記憶、入出力の管理を行なうために、

- 5 (1) 他の装置（ライセンス提供装置または他のHD）からライセンスの提供を受けて格納する書込処理（図9および図10におけるHD20および図21～図23におけるHD21の処理）
- (2) 書込処理の中止から、書込処理を再開する再書込処理（図13～図15におけるおけるHDおよび図21～図23におけるHD21の処理）
- 10 (3) 他のHDに対してライセンスを移動または複製する提供処理（図16～図18におけるHD20の処理）
- (4) 提供処理の中止から、移動複製処理を再開する再提供処理（ライセンスの提供元としての再書込処理、図21～図23におけるHD20の処理）
- (5) 暗号化コンテンツデータを復号することを目的として再生回路に対してコ

15 ンテンツ鍵Kcを提供する再生許諾処理（図24におけるHD20の処理）

の5つの処理を、暗号技術によって実現している。

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

#### [実施の形態2]

実施の形態1においては、HD20は、図13～図15のフローチャートに示される再書込処理および図21～図23のフローチャートに示される再提供処理において、再書込／提供処理を開始するにあたって、処理の可否を判断するために、再書込／提供処理の対象となるライセンスに対する直前のログを検索する。そして、対応したログが検索された場合、検索したログをログメモリ253のバンクnに複製して、以後の処理においてはバンクnに格納されたログを処理の手順に従って更新していくものとして説明した。

しかし、再書き込み処理においては、複製したログはライセンスの提供側に対して直前の処理に対するログとして出力した後、図14のステップS137において、その内容が書き換えられてしまう。ログの複製は、古いログが格納されたバンクから順に新たなログの格納バンクに向けて循環的に使用していくログメモリ253の特性に由来するものであり、再書き込み処理の初期における中断（図14のステップS136以前）においても、再書き込み処理に対応するログが、より長くログメモリ253に保持されることを目的としている。

したがって、十分に大きなログメモリ253を備えたHDにおいては、再書き込み処理における検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接出力するように構成することも可能である。この場合、ステータスST2の変更（ステップS115, S116, S117）は、当該バンクのログに対して行なわれ、出力するためのログの取得（ステップS118）は、当該バンクから行なわれることとなる。

また、ログの複写がなされないため、再書き込み処理に対応するログを格納するためのバンクは、図14のステップS137において確保される。したがって、ステップS137は、「ログメモリの最も古いログを格納しているバンクn<sub>a</sub>に新たなログを格納」と変更される。

さらに、HD21も同様に処理を変更することが可能である。その他の全ての処理は、実施の形態1と同じである。なお、この処理の変更によってライセンスの安全性は何ら変化することなく、実施の形態1と同様の効果を得ることができる。

### 〔実施の形態3〕

ライセンスの再書き込み処理と同様に、ライセンスの再提供処理において、検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接読み出し、再提供の可否を判定することも可能である。図21のステップS301aにおいて複製を行なうことなく、図21のステップS302および図22のステップS329, S331, S332において検索されたログが格納されていたバンクから直接ログを取得するように処理を変更すればよい。その他の全ての処理は、実施の形態1と同じである。

この処理の変更によってライセンスの安全性は、何ら変化することではなく、実施の形態1と同様の効果を得ることができる。また、実施の形態2と組合わせることも可能である。

〔実施の形態4〕

5 HD 20の実装における処理を軽減するためには、通常の書込処理および再書込処理は、より共通していることが望ましい。そこで、実施の形態1における「セッション鍵要求」移行のHD 20における処理、すなわち、通常の書込処理（図9のステップS19～S22、図10のステップS33～S35, S38～S43）と再書込処理（図14のステップS136～S139、図15のステップS150～S152, S154～S160）を共通とする。この場合、図9のステップS20と図14のステップS137とを同一処理とすることで容易に実現できる。

10

この場合、ステップS137をステップS20と同一処理とし、“ログメモリの最も古いログを格納しているバンクn bに新たなログを格納”とする。また、詳細な処理は、図11および図12のフローチャートに従い、変数nを変数n bと読み替える。また、変数nを変数n bと読み替えるのは、図13および図14のステップS137までの処理における変数nと区別するためである。これに伴って、図14および図15のステップS137以降のステップS154, S155, S159におけるバンクnを全てバンクn bと読み替える。

15

20 同様に、移動複製セッションでは、図21～図23のフローチャートに示されるステップS342以降の処理と、図16～図18のフローチャートに示されるステップS222以降の処理との違いが、ログの記録の違い（図23のステップS345と図18のステップS225との違い）のみである。図23のステップS345の処理を図18のステップS225と同一の処理とすることによってHD 20の実装を容易にすることができます。この場合、ステップS345をステップS20と同一処理とし、“ログメモリの最も古いログを格納しているバンクn bに新たなログを格納”とする。また、詳細な処理は、図20および図12のフローチャートに従い、変数nを変数n bと読み替える。また、変数nを変数n bと読み替えるのは、図21および図22のステップS245までの処理における

25

る変数  $n$  と区別するためである。これに伴って、図 2 3 のステップ S 3 4 5 以降のステップ S 3 4 8, S 5 7 におけるバンク  $n$  を全てバンク  $n$  b と読み替える。

その他の全ての処理は、実施の形態 1 と同一である。また、処理の変更によってライセンスの安全性は何ら変化することなく、実施の形態 1 と同様な効果を得ることができる。さらに、HD 2.1 も同様に処理を変更することが可能である。

このように、通常書込処理および再書込処理の共通化によって、実施の形態1と同様なライセンスの安全な管理を実現した上で実装する処理量の軽減を図ることができる。

### [実施の形態 5]

ログの記録開始タイミングを明確にするために、全ての処理においてHD外部からライセンスID（LID）を受理することによって、ログメモリ253からバンクを1つ確保し、当該処理に対するログを記録するように変更した実施の形態5について説明する。

まず、実施の形態5におけるライセンスの配信動作について説明する。

実施の形態5においては、ライセンス提供措置40からHD20へのライセンスの配信は、図25および図26に示すフローチャートに従って行なわれる。図25および図26に示すフローチャートは、図9および図10に示すフローチャートのステップS16とステップS17との間にステップS16aを挿入し、ステップS20をステップS201aに代えたものであり、その他は図9および図10に示すフローチャートと同じである。

ステップS16aの詳細な動作は、図27に示すフローチャートに従って行なわれる。図27を参照して、HD20にコントローラ214は、ステップS16の後、最新のログが格納されているバンクn-1を特定し、バンクnに格納されている管理番号mを取得する（ステップS16b）。そして、このステップS16bの詳細な動作は、図12に示すフローチャートに従って行なわれる。

コントローラ 214 は、ステップ S16b の後、管理番号  $m+1$ 、およびステップ S16 で受理したライセンス ID (LID) をバンク  $n$  に格納し、バンク  $n$  に格納されたログの ST1 領域 2544 を“受信待”に設定する (ステップ S16c)。これにより、図 25 に示すステップ S16a の動作が終了する。

また、コントローラ 214 は、ステップ S19 の後、ログメモリ 253 のバンク n に格納されたログの Ks2x 領域 2543 に、ステップ S19 で受理したセッション鍵 Ks2a を記録する（ステップ S201a）。

その他は、実施の形態 1 において説明したとおりである。

5 [配信における再書き込み]

実施の形態 5 におけるライセンスの配信が途中で中断した場合のライセンスの再書き込み動作は、図 13～図 15 に示すフローチャートに従って行なわれる。その詳細な動作は実施の形態 1 において説明したとおりである。

[移動／複製]

10 図 28 および図 29 は、図 17 に示すライセンスの複製・移動が可能なシステムにおいて、端末装置 10 のユーザが端末装置 10 から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置 10 を介して端末装置 10 に装着された HD20 から HD21 へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための実施 15 の形態 5 における第 1 および第 2 のフローチャートである。

図 28 および図 29 に示すフローチャートは、図 18 および図 19 に示すフローチャートのステップ S207 とステップ S209 との間にステップ S208 を挿入し、ステップ S214 とステップ S215 との間にステップ S214a を挿入し、ステップ S218 をステップ S218a に代え、ステップ S225 をステップ S225a に代えたものであり、その他は図 18 および図 19 に示すフローチャートと同じである。

20 図 28 を参照して、HD20 のコントローラ 214 は、ステップ S207 において HD21 からの証明書 Cm1 を承認したとき、ログメモリ 253 のうち最も古いログが格納されたバンク n に新たなログを格納する（ステップ S208）。このステップ S208 の詳細な動作は、図 30 に示すフローチャートに従って行 25 なわれる。

25 図 30 を参照して、ステップ S208 は、HD20 においてログメモリ 253 の最新ログが記録されたバンク n-1 を特定し、かつ、バンク n-1 に格納された管理番号 m を取得するステップ S208a と、バンク n に、管理番号 m+1、

ライセンス I D (L I D) 、およびクラス公開鍵 K P c m y を格納し、かつ、 S T 1 領域 2 5 4 4 のステータス S T 1 を“送信待”に設定するステップ S 2 0 8 b とから成る。そして、ステップ S 2 0 8 a の詳細な動作は、図 1 2 に示すフローチャートに従って行なわれる。したがって、コントローラ 2 1 4 は、図 1 2 および図 3 0 に示すフローチャートに従って、ステップ S 2 0 6 において受理したライセンス I D (L I D) と HD 2 1 のクラス公開鍵 K P c m 1 と、“送信待”に設定されたステータス S T 1 とを記録した新たなログをバンク n に格納する。

また、 HD 2 1 のコントローラ 2 1 4 は、ステップ S 2 1 4 の後、最も古いログが格納されたバンク n a に新たなログを格納する (ステップ S 2 1 4 a) 。このステップ S 2 1 4 a の詳細な動作は、上述した図 1 2 および図 2 7 に示すフローチャートに従って行なわれる。ただし、変数 n は、変数 n a に読み替える。

したがって、 HD 2 1 のコントローラ 2 1 4 は、図 1 2 および図 2 7 に示すフローチャートに従って、ステップ S 2 1 4 において受理したライセンス I D (L I D) と、“受信待”に設定されたステータス S T 1 とを記録した新たなログを、ログメモリ 2 5 4 の中で最も古いログが格納されていたバンク n a に格納する (ステップ S 2 1 4 a) 。

さらに、 HD 2 1 のコントローラ 2 1 4 は、ステップ S 2 1 7 の後、ログメモリ 2 5 3 のバンク n a にステップ S 2 1 7 において生成されたセッション鍵 K s 2 a を格納する (ステップ S 2 1 8 a) 。

さらに、 HD 2 0 のコントローラ 2 1 4 は、ステップ S 2 2 4 の後、ログメモリ 2 5 3 のバンク n に、ステップ S 2 2 4 で受理したセッション鍵 K s 2 a を格納する (ステップ S 2 2 5 a) 。

その他は、実施の形態 1 において説明したとおりである。

#### [移動／複製における再書き込み]

実施の形態 5 における HD 2 1 から HD 2 0 へのライセンスの移動・複製セッションが途中で中断した場合のライセンスの再書き込み動作は、図 2 1 ～図 2 3 に示すフローチャートに従って行なわれる。したがって、その詳細な動作は実施の形態 1 で説明したとおりである。

このように、実施の形態 5 では、実施の形態 1 と同様に安全なライセンスの再

書込／提供処理を実現し、かつ、それぞれの処理におけるログの発生タイミングを明確にするとともに、実施の形態3と同様に、通常書込／再書込処理の共通化によって実装する処理量の軽減を図ることができる。なお、HD21も同様に処理を変更することが可能である。

5 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内のすべての変更が含まれることが意図される。

#### 10 産業上の利用可能性

この発明は、機密データの入出力処理に関する履歴情報を重複することなく複数格納できるデータ記憶装置に適用可能である。

## 請求の範囲

1. 一定の手順に従って機密データの入出力を行ない、前記機密データを記憶し、かつ、前記一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置（20）であって、

外部とデータの入出力を行なうインターフェース（212）と、

複数の前記機密データを格納するデータ記憶部（270）と、

前記機密データの入出力に関する複数の履歴情報を格納するログ記憶部（253）と、

前記機密データの入出力を制御する制御部（214）とを備え、

前記ログ記憶部（253）は、それぞれ1つの前記履歴情報を格納する2つ以上の領域を循環的に利用するリングバッファとして設けられており、

前記ログ記憶部（253）に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、

前記制御部（214）は、前記機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報を前記インターフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記ログ記憶部（253）に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に前記受取った識別情報を含む前記機密データの入出力処理に対する履歴情報を新たに格納する、データ記憶装置。

2. 履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報を前記インターフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、前記最新領域に格納されている履歴情報の一部または全てを前記インターフェース（212）を介して出力する、請求の範囲第1項に記載のデータ記憶装置。

3. 履歴情報の出力を伴う前記機密データの入力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報を前記インターフェース（212）を介して受取り、前記ログ記憶部（253）の複数の領域（2531～253N）を所定の順序で検索して、前記最古領域と、前記受け取った識別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの入力処理に対する新たな履歴情報として格納し、前記特定された最古領域に格納された履歴情報の一部または全てを前記インターフェース（212）を介して出力する、請求の範囲第1項に記載のデータ記憶装置。

4. 他の装置によって前記一定の手順の進行によって記録されたもう1つの履歴情報の入力を伴う前記機密データの再出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報および前記もう1つの履歴情報を前記インターフェース（212）を介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納された履歴情報と、前記受け取ったもう1つの履歴情報に基づいて、前記機密データを出力するか否かを判定する、請求の範囲第2項または請求の範囲第3項に記載のデータ記憶装置。

5. 他の装置によって前記一定の手順の進行に従って記録されたもう1つの履歴情報の入力を伴う前記機密データの出力処理において、

前記制御部（214）は、入出力の対象となる機密データの識別情報および前記もう1つの履歴情報を前記インターフェース（212）を介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの出力処理に対する新たな履歴情報として格納し、前記特定した最古領域に格納された履歴情報と、前記受け取ったもう1つの履歴情報に基づいて、前記機密データを出力するか否かを判定する、請求の範囲第2項または請求の範囲第3項に記載のデータ記憶装置。

6. 前記最古領域を特定した後、

前記制御部（214）は、前記入出力処理における一定の手順が終了あるいは中止されるまでの間、前記特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する、請求の範囲第1項に記載のデータ記憶装置。

7. 前記複数の履歴情報の各々は、前記ログ記憶部（253）へ記憶された順序を識別するための管理番号（2541）をさらに含み、

前記管理番号（2541）は、前記ログ記憶部（253）に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される前記最古領域を検出する、請求の範囲第1項に記載のデータ記憶装置。

10 8. 前記ログ記憶部（253）は、N（Nは2以上の自然数）個の領域（253  
1～253N）を循環的に利用するリングバッファからなり、

前記管理番号（2541）は、M（Mは、N<Mを満たす自然数）の剩余系からなる、請求の範囲第7項に記載のデータ記憶装置。

9. 前記制御部（214）は、前記ログ記憶部（253）に連続して配置された  
15 2つの領域に格納された2つの履歴情報に含まれる各々の管理番号（2541）  
を取得し、その取得した2つの管理番号（2541）の差に基づいて、2つの当  
該管理番号（2541）を含む2つの履歴情報が連続して格納されたか否かを判  
定し、2つの履歴情報が不連続に格納された履歴情報であるとき、前記連続する  
2つの領域のうち、後続領域を前記最古領域として検出する、請求の範囲第8項  
20 に記載のデータ記憶装置。

FIG. 1

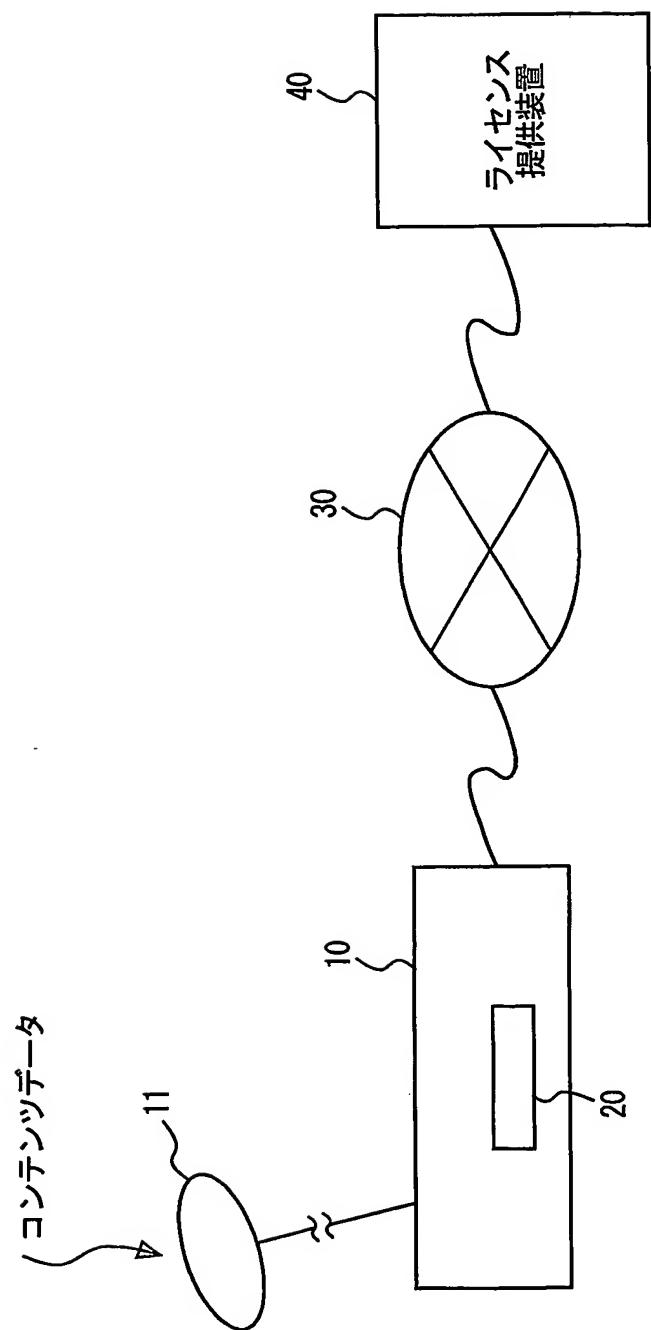


FIG. 2

記号	名称	属性	特性
Dc	データ	データ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて暗号化した暗号化データコンテンツデータ、記録管理される E(Kc, Dc)
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

## FIG. 3

記号	名称	特性
KPa	認証鍵	認証局にて証明書を検証する公開復号鍵
Ks1x	セッション鍵	ライセンス提供側にて運用される一時鍵 共通鍵
Ka	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵
KPa	認証鍵	認証局にて運用される一時鍵 ライセンス提供側にて運用される一時鍵
KPcmY	クラス公開鍵	機器のクラス(種類などの一一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
KcmY	クラス秘密鍵	クラス公開鍵(KPcmY)にて暗号化されたデータを復号する非対称な復号鍵
IcmY	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
GmY	クラス証明書	Cmy=KPcmY//IcmY//E(Ka,H(KPcmY//IcmY)) 認証鍵KPaによってその正当性が確認できる
KPomZ	個別公開鍵	データ記録装置ごとに固有名を持つ個別公開暗号鍵
KomZ	個別秘密鍵	「z」はデータ記録装置を識別するための識別子
Ks1x	セッション鍵	個別公開鍵(KPomZ)にて暗号化されたデータを復号する非対称な復号鍵 ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵
KPcpY	クラス公開鍵	機器のクラス(種類などの一一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
KcpY	クラス秘密鍵	クラス公開鍵(KPcpY)にて暗号化されたデータを復号する非対称な復号鍵
IcpY	クラス情報	Cpy=KPcpY//IcpY//E(Ka,H(KPcpY//IcpY)) 認証鍵KPaによってその正当性が確認できる
Cpy	クラス証明書	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵
Ks2x	セッション鍵	

FIG. 4

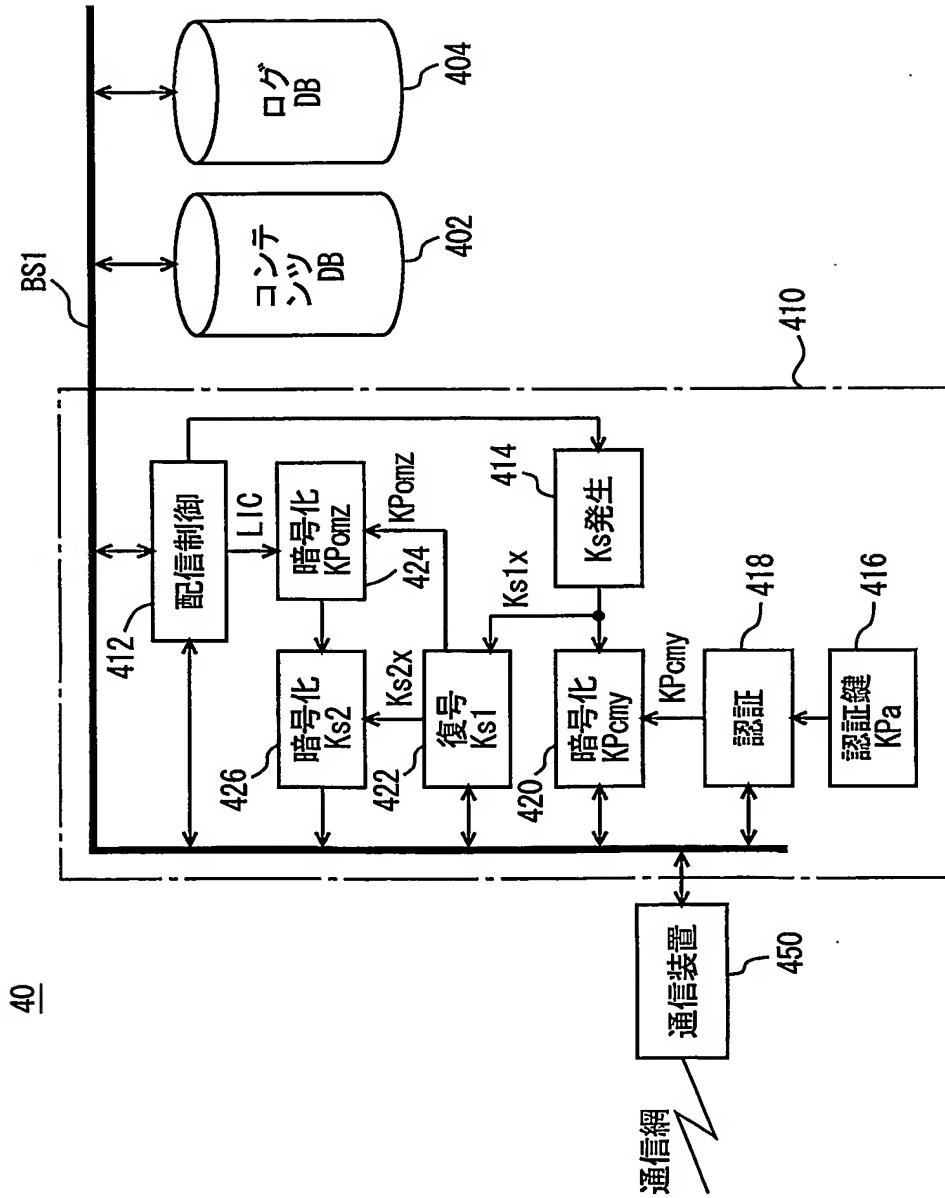
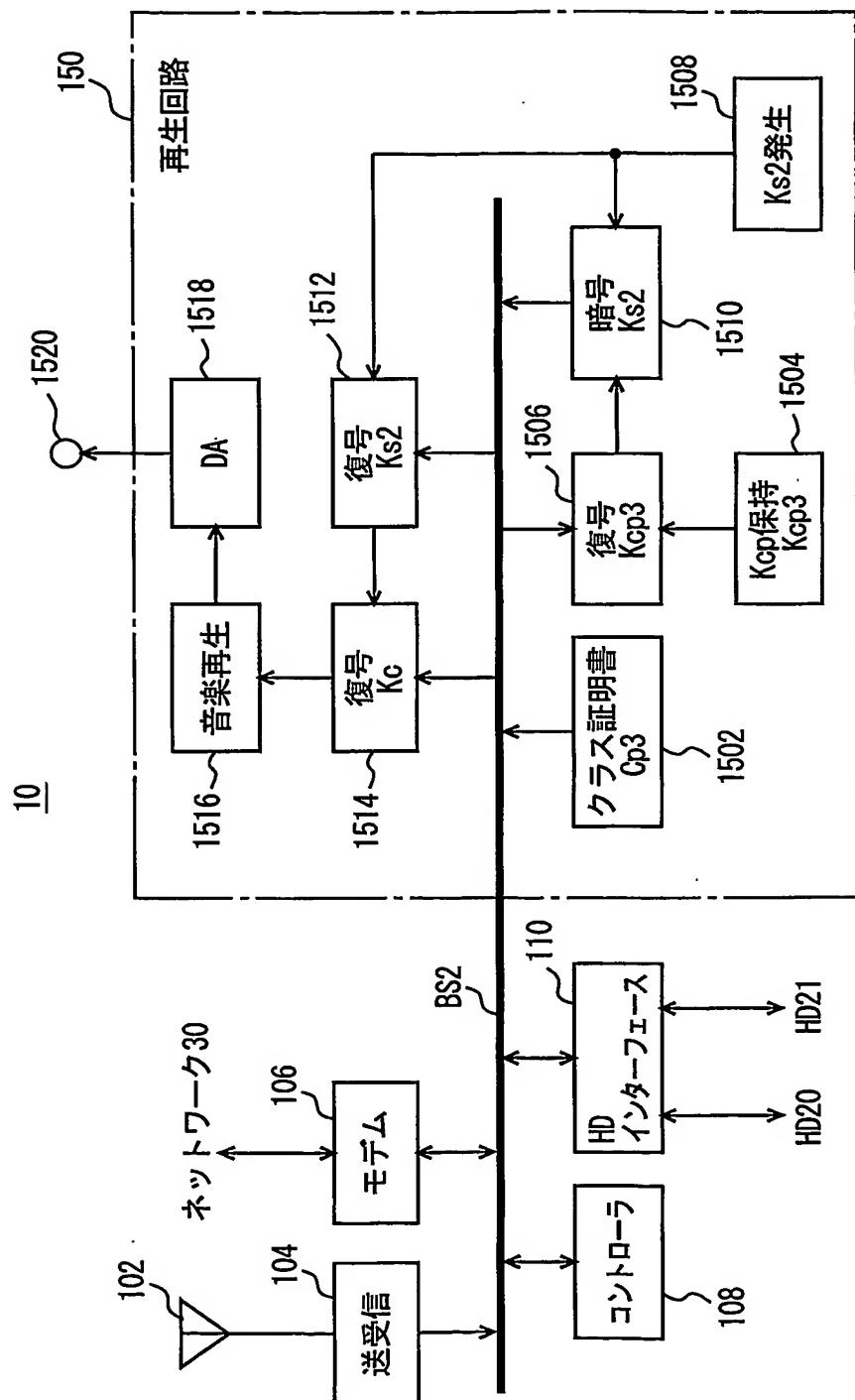


FIG. 5



6  
FIG.

20, 21

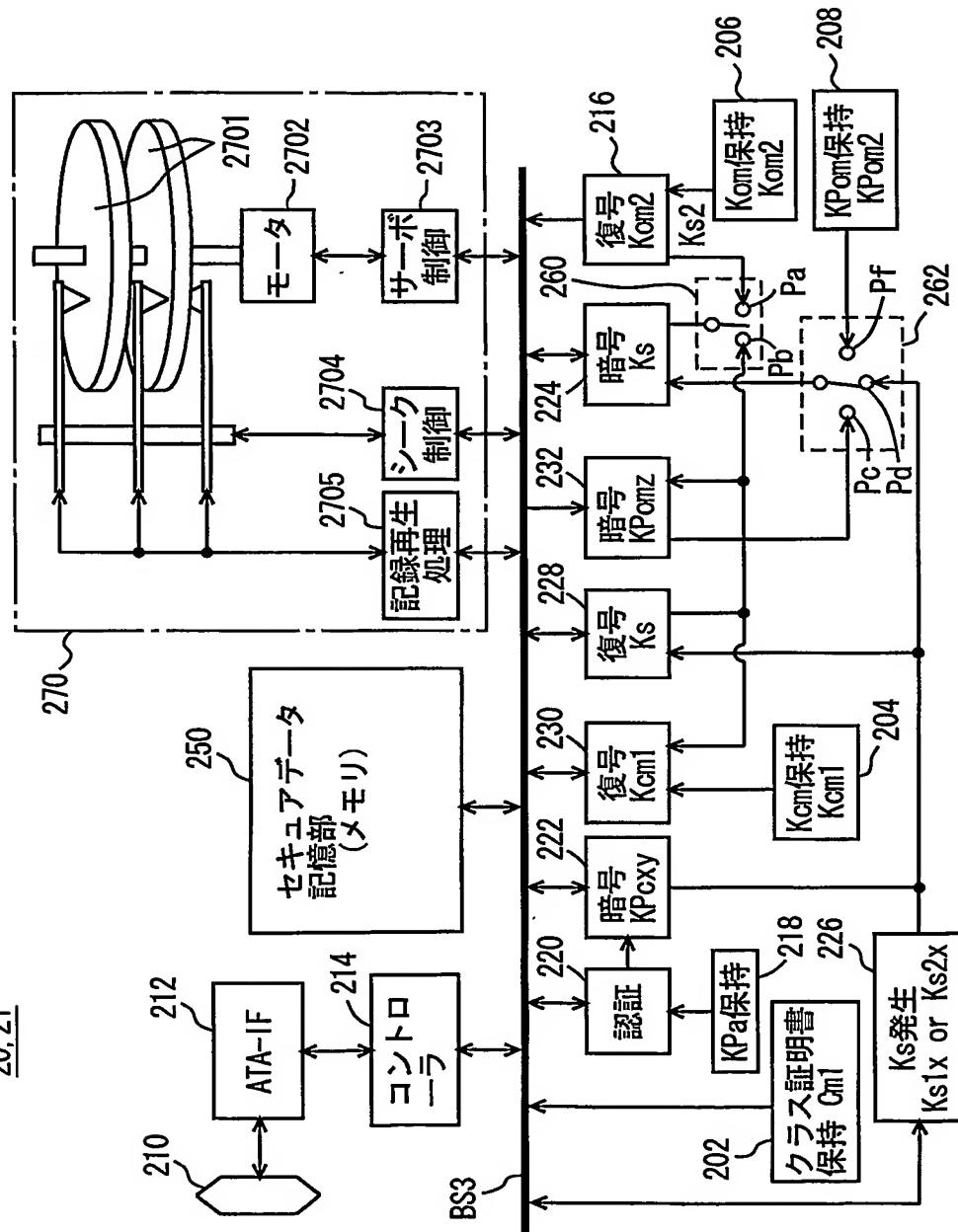


FIG. 7

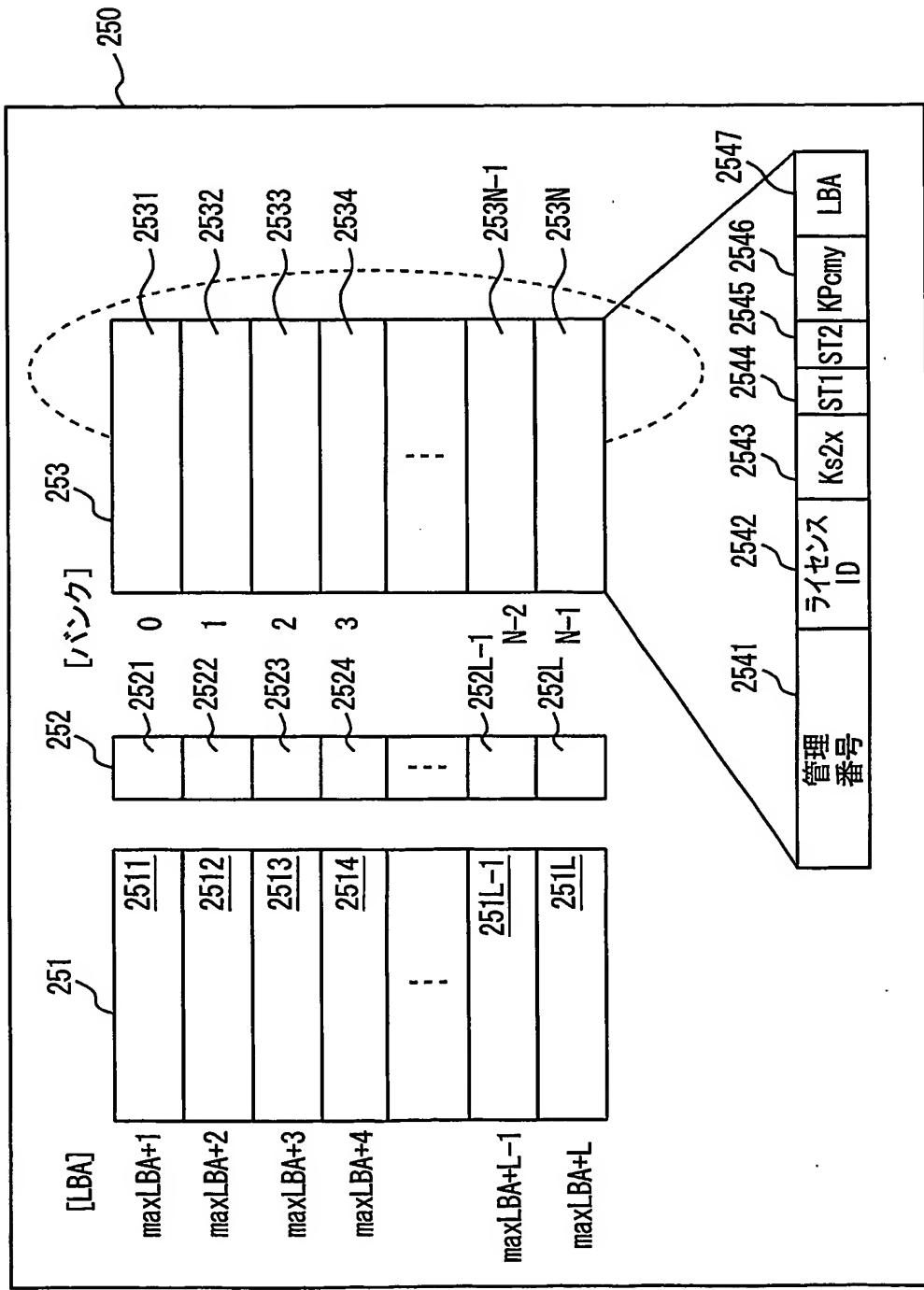
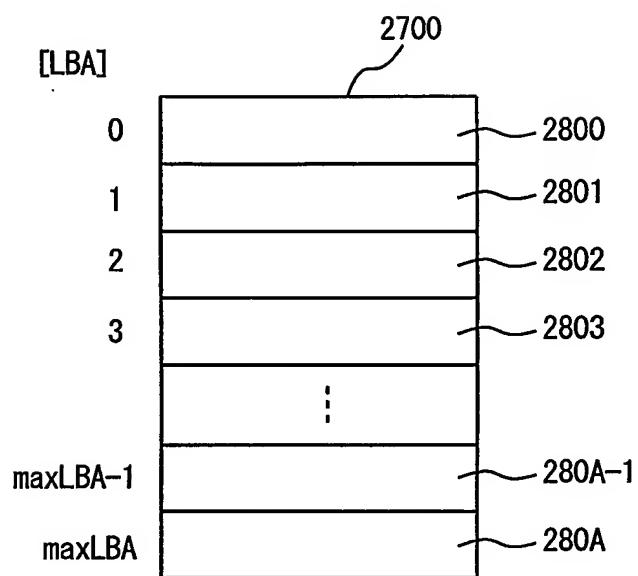


FIG. 8



## FIG. 9

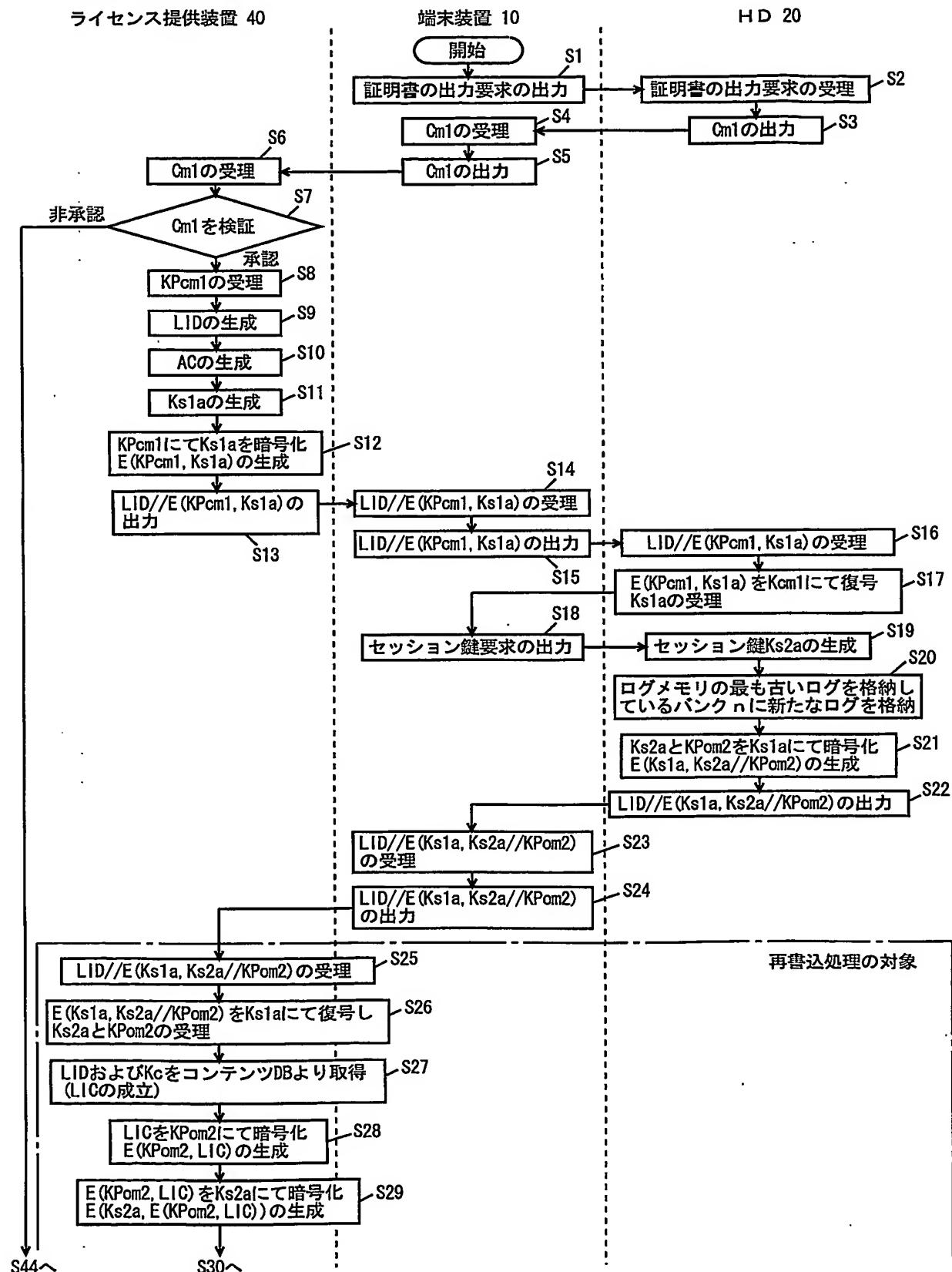


FIG. 10

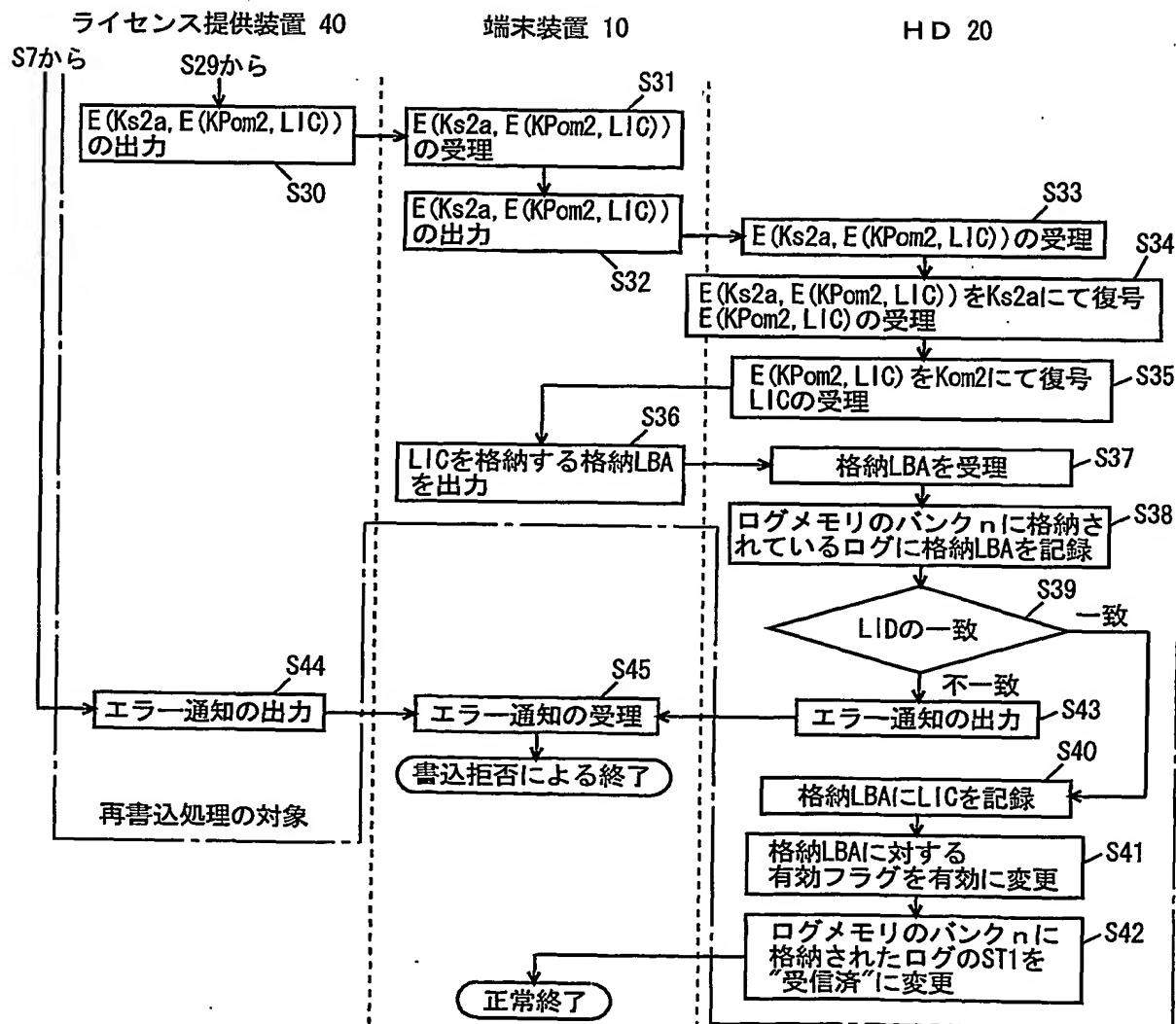


FIG. 11

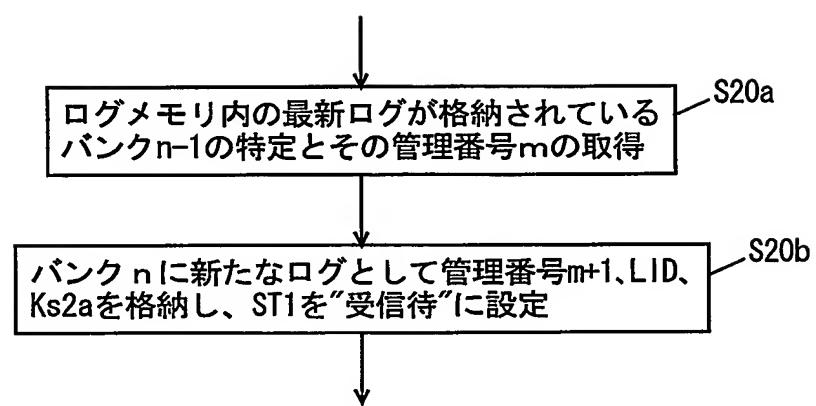


FIG. 12

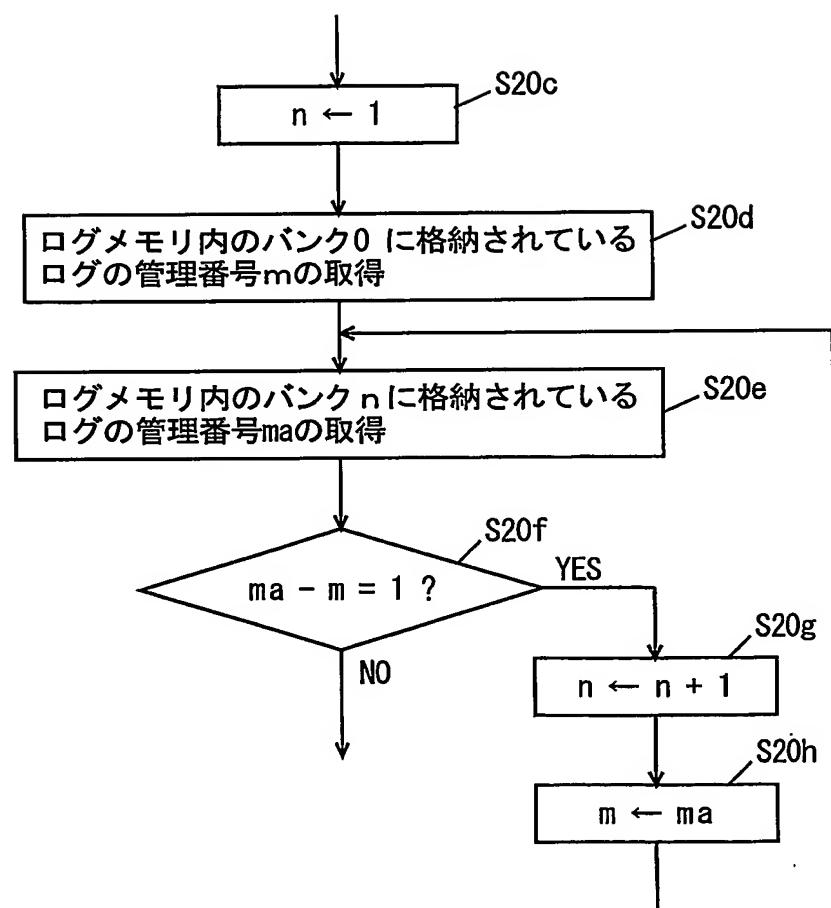
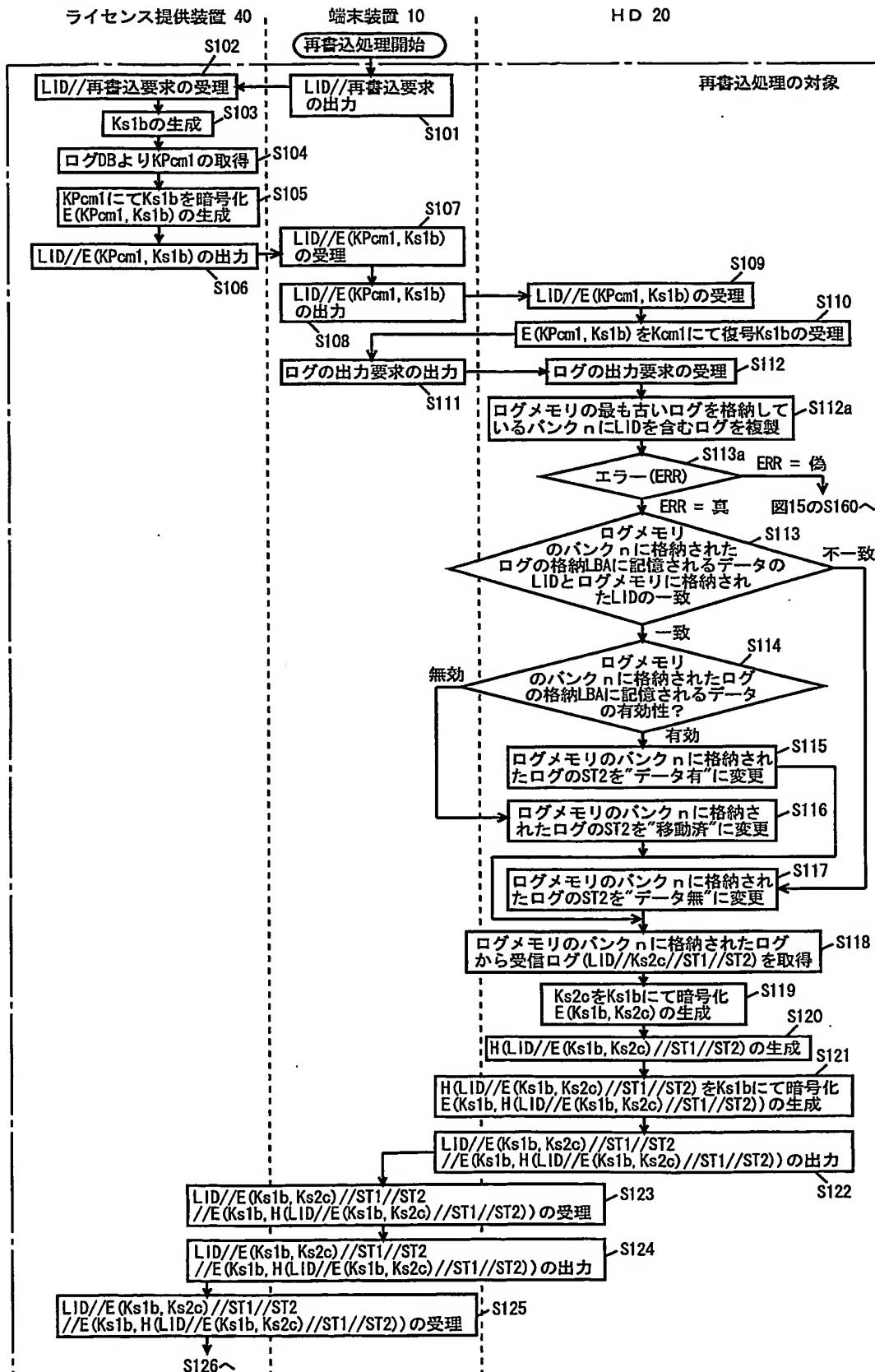


FIG. 13



## FIG. 14

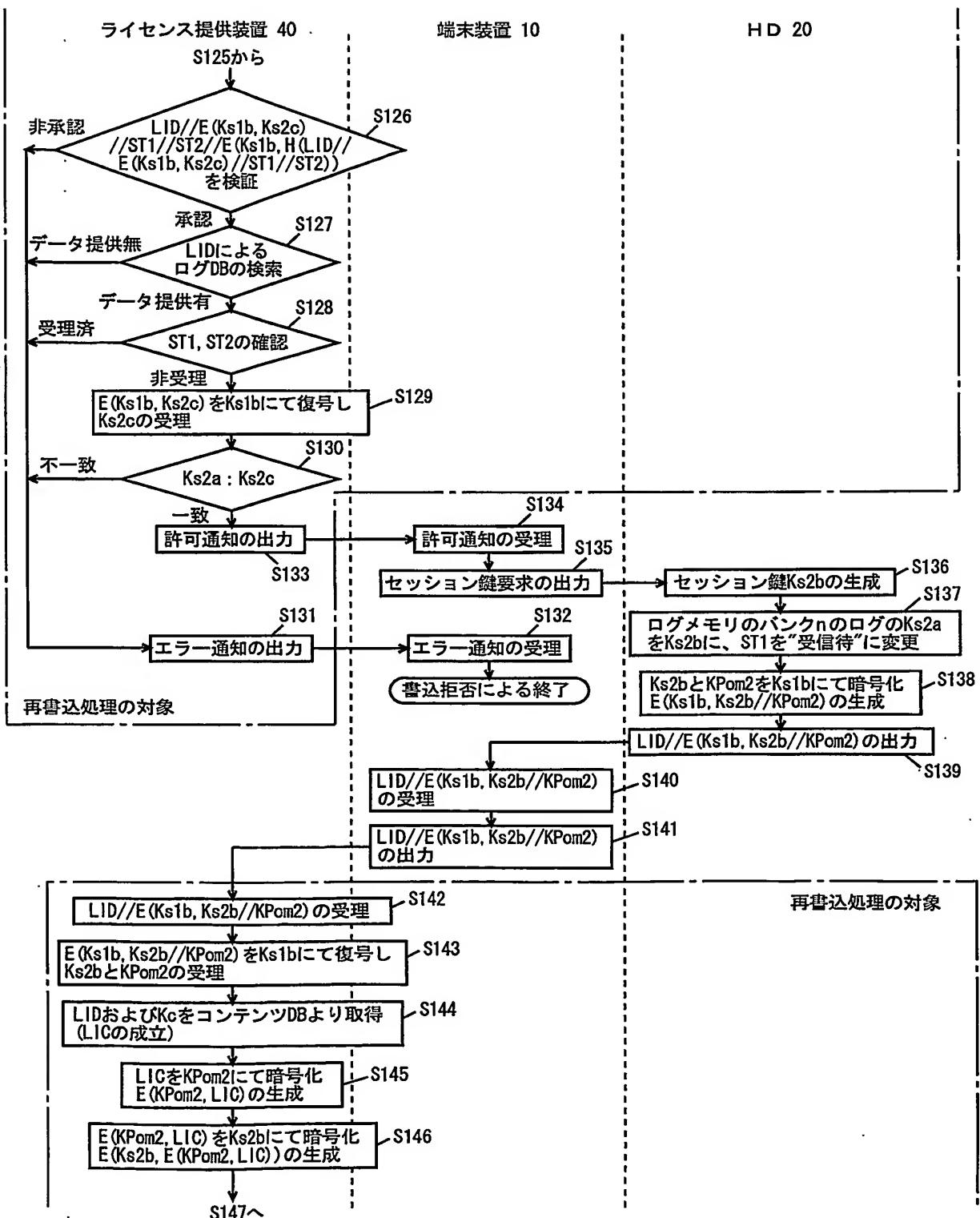


FIG. 15

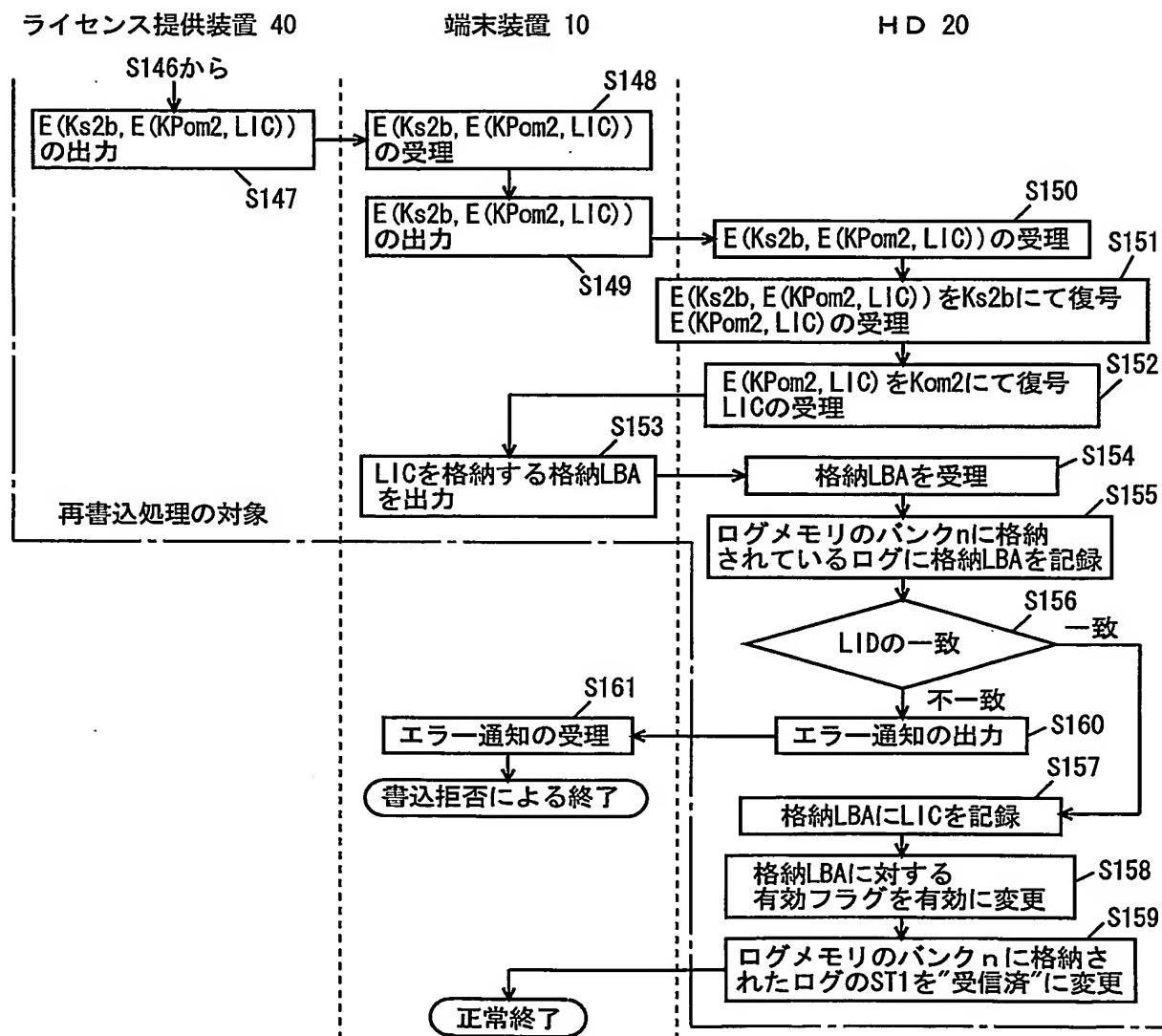
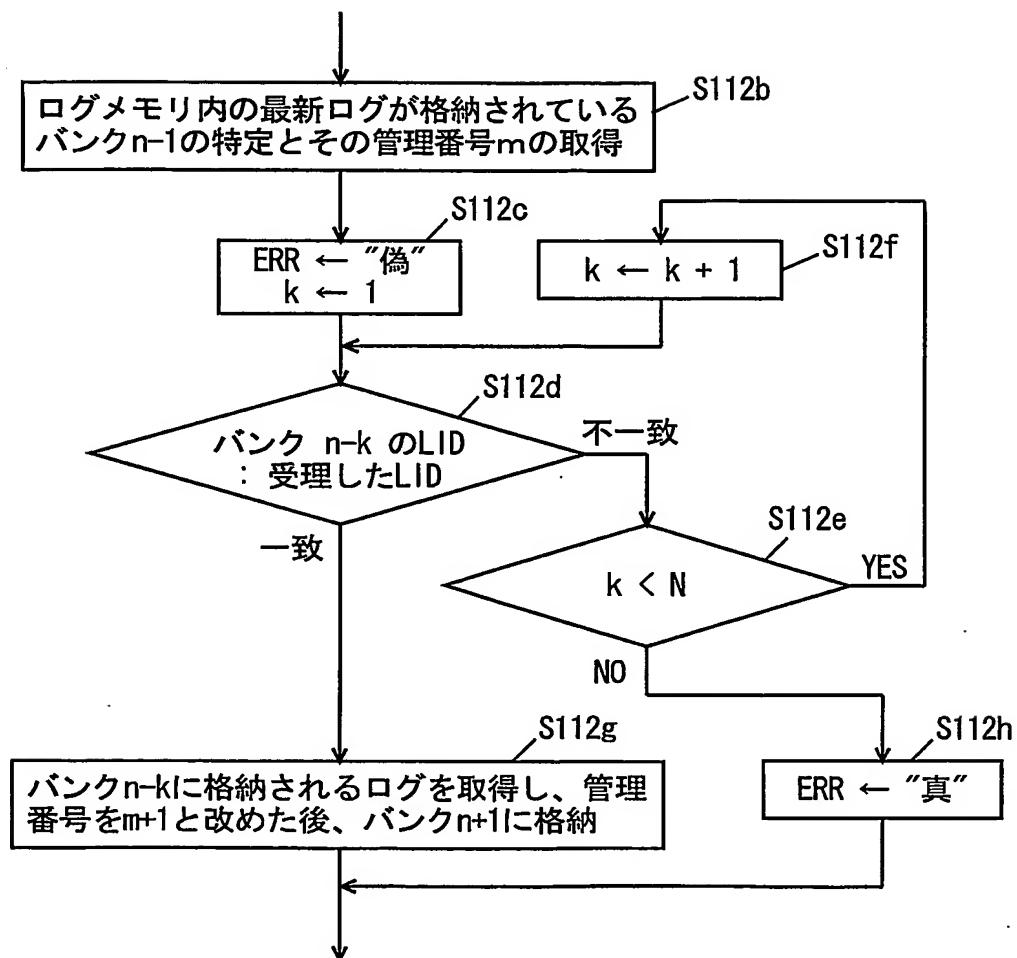


FIG. 16



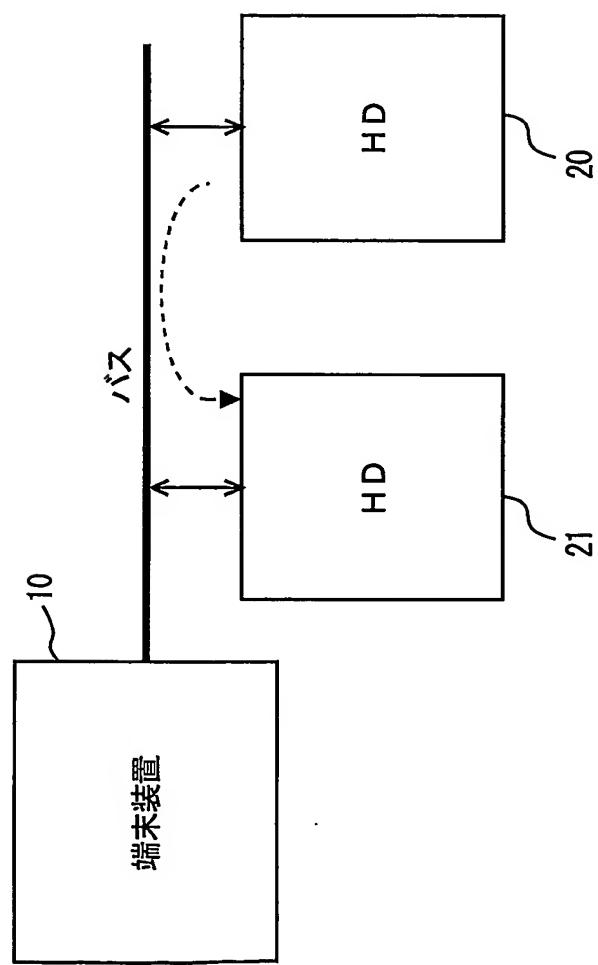


FIG. 17

## FIG. 18

HD 20

HD 21

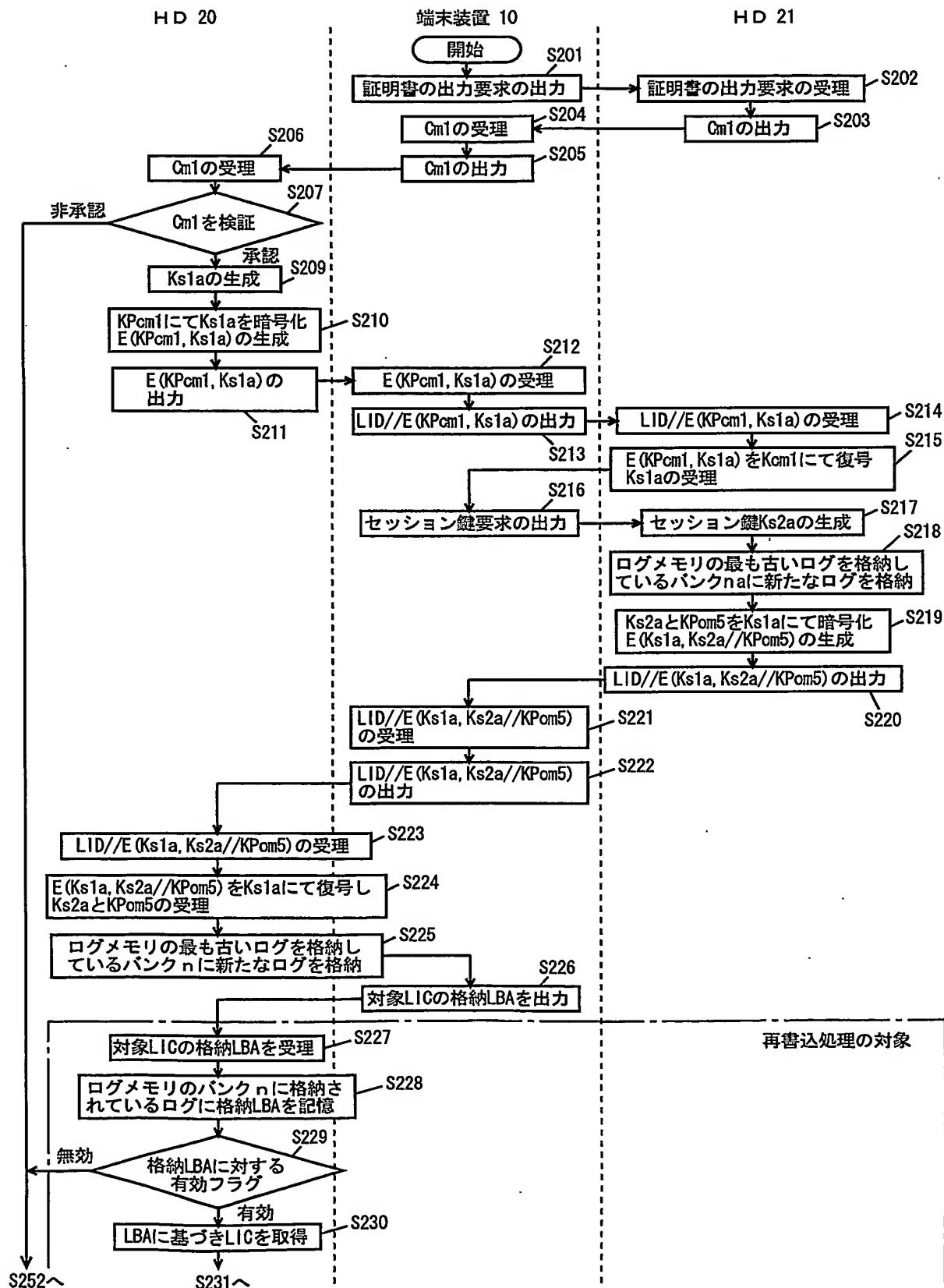


FIG. 19

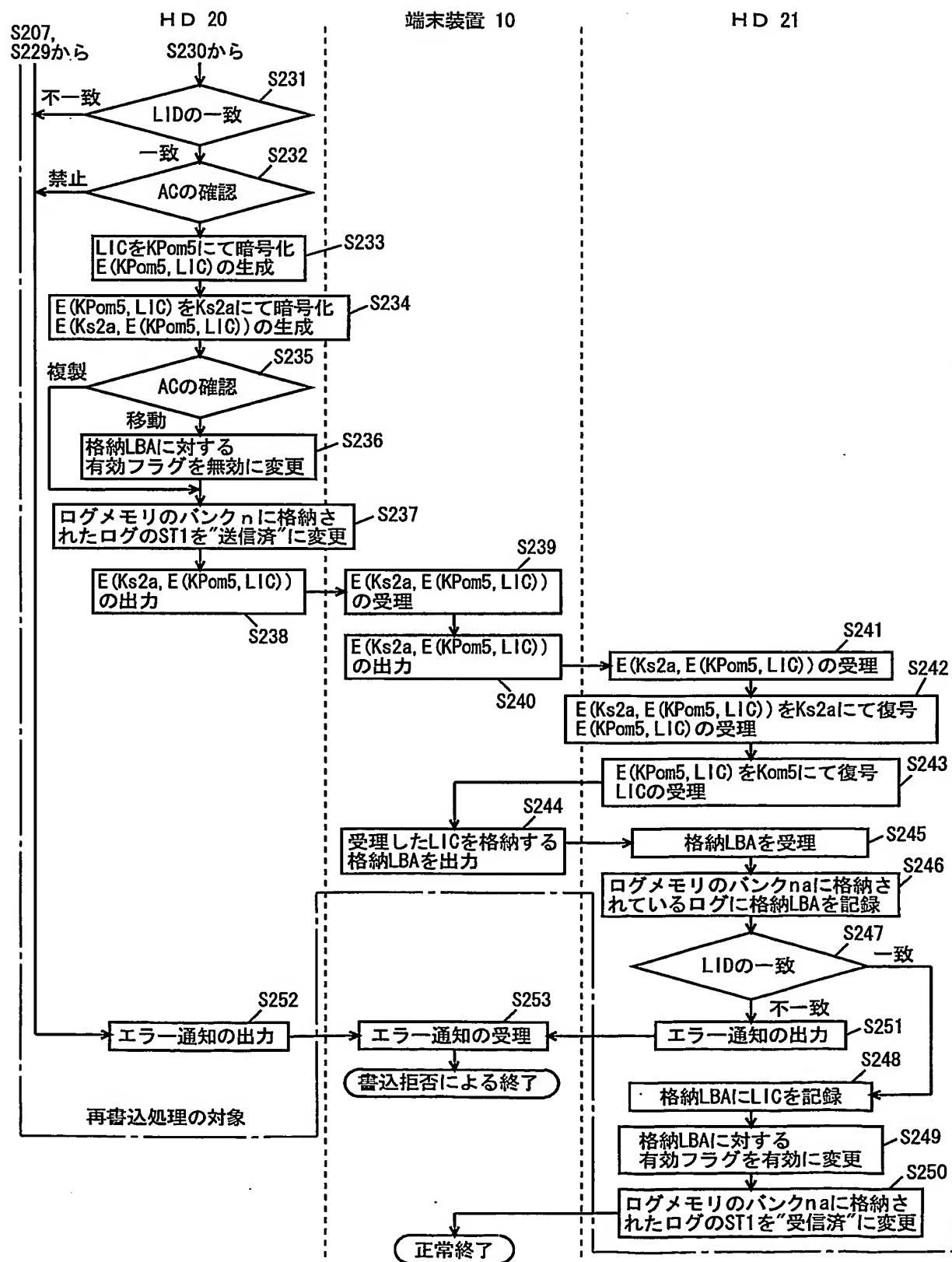
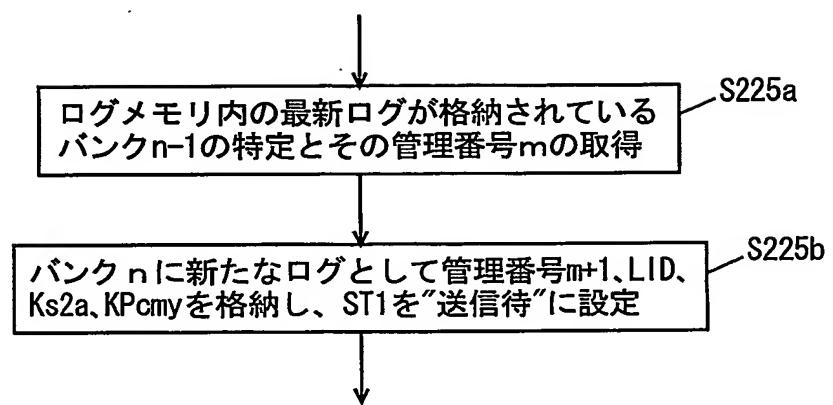


FIG. 20



F I. G. 2 1

H D 20

H D 21

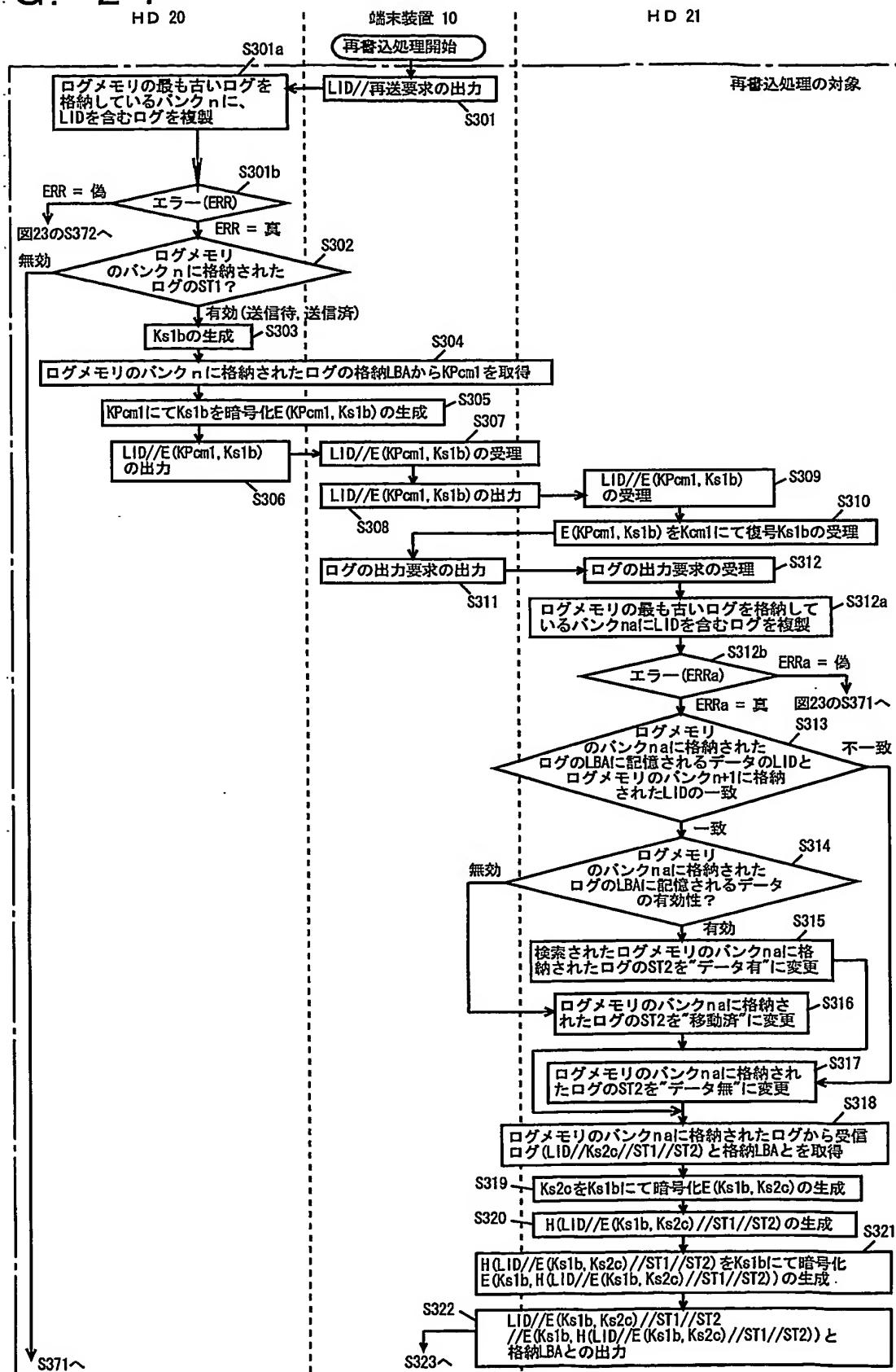


FIG. 22

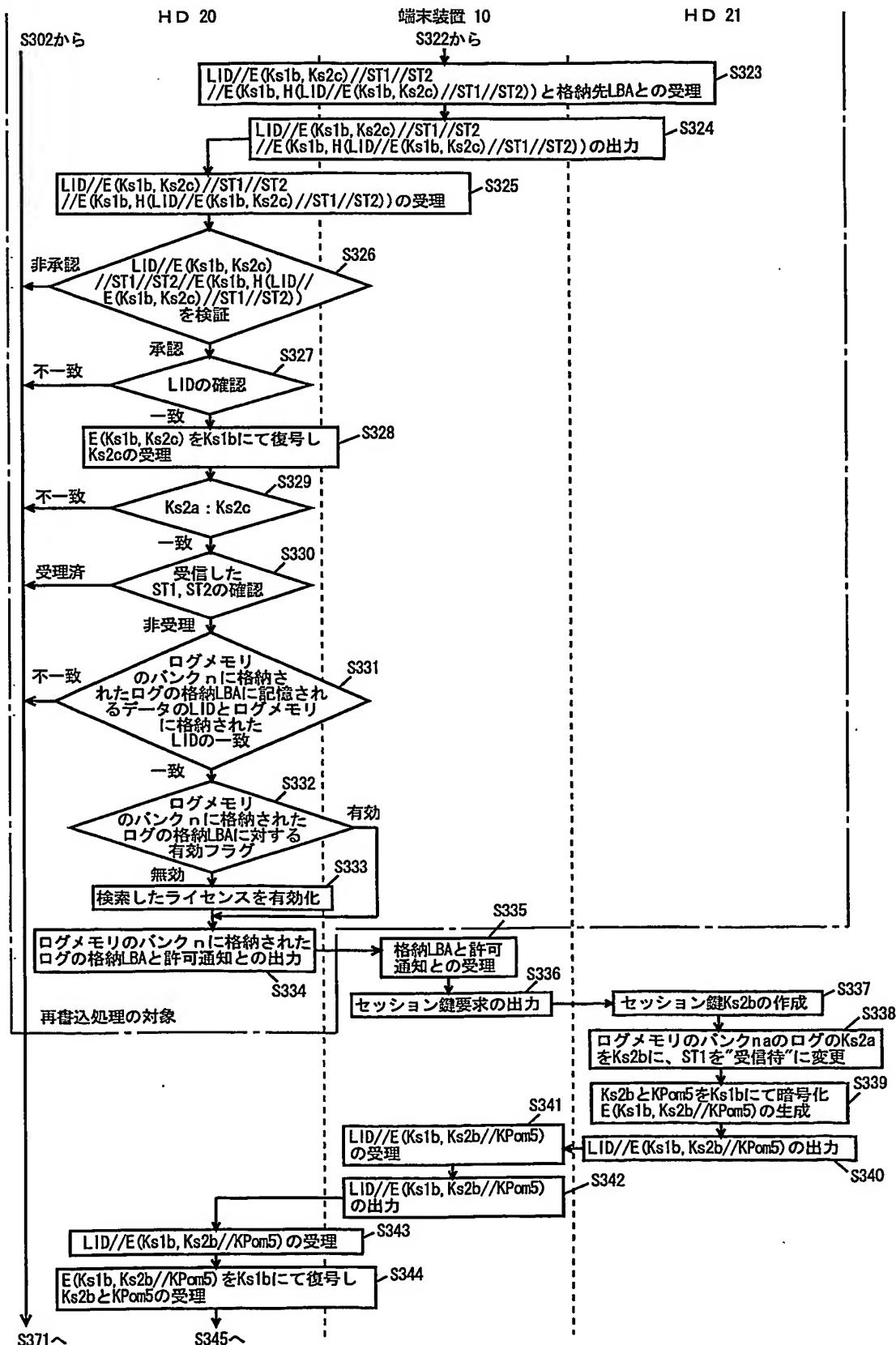


FIG. 23

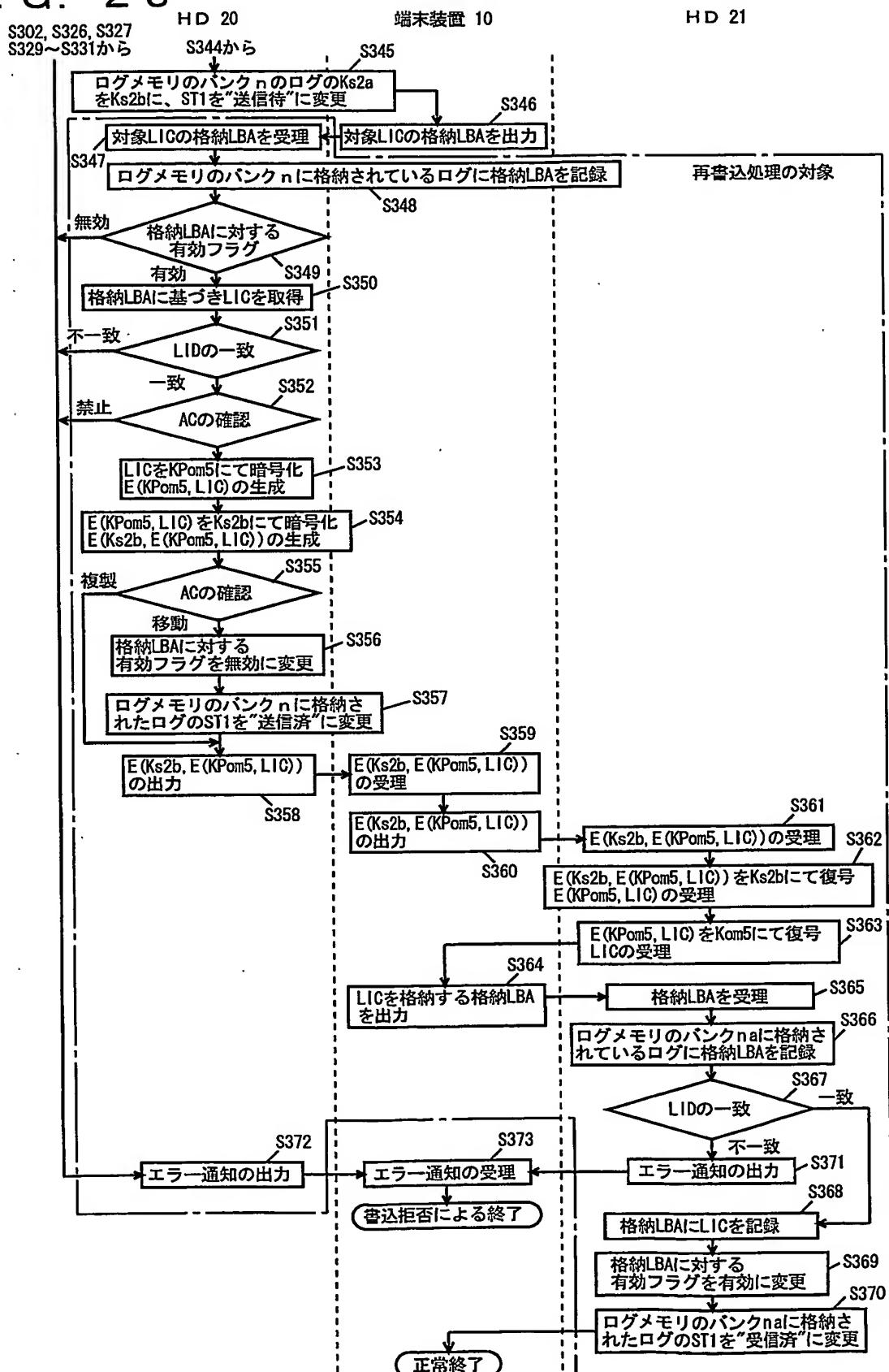


FIG. 24

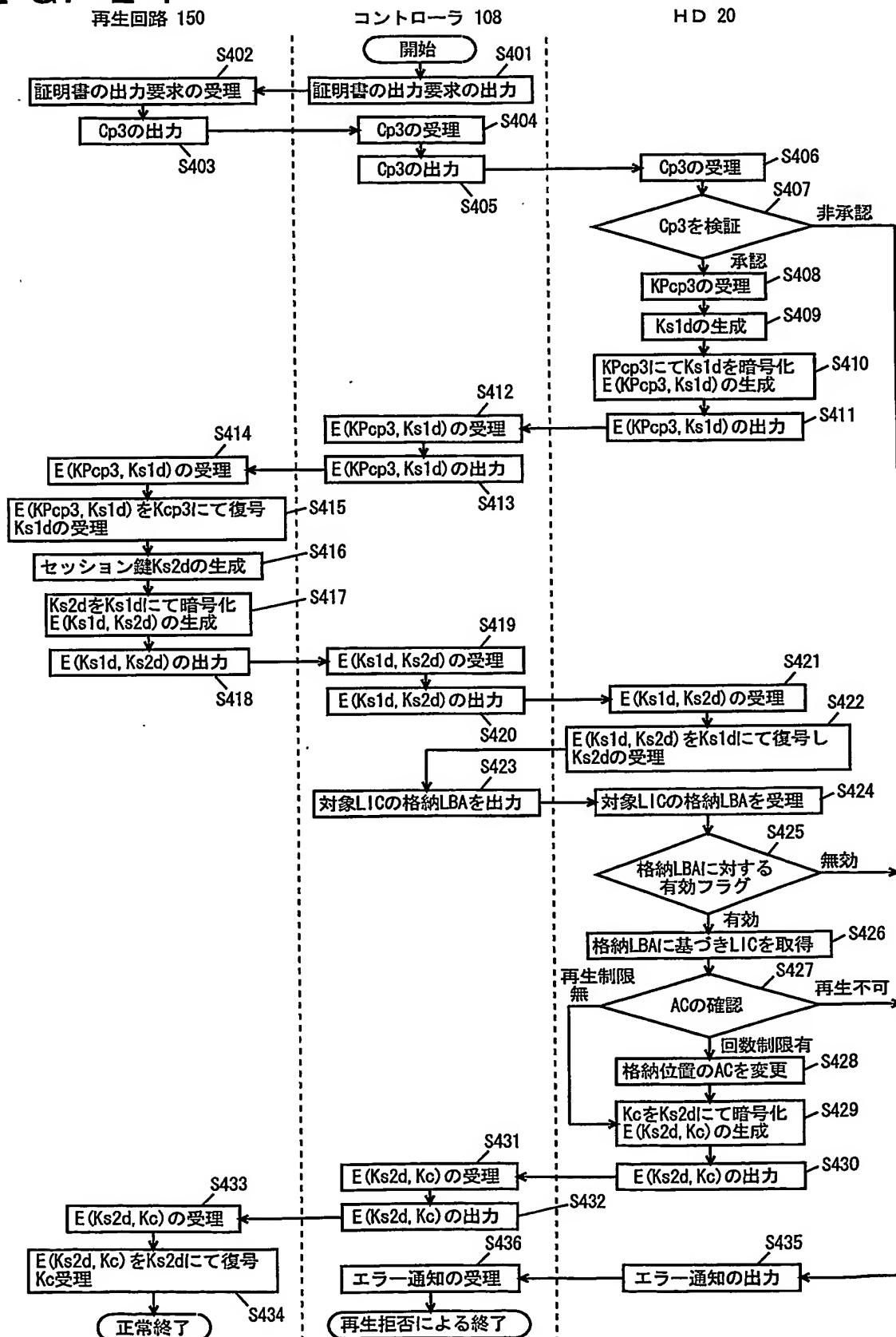


FIG. 25

ライセンス提供装置 40

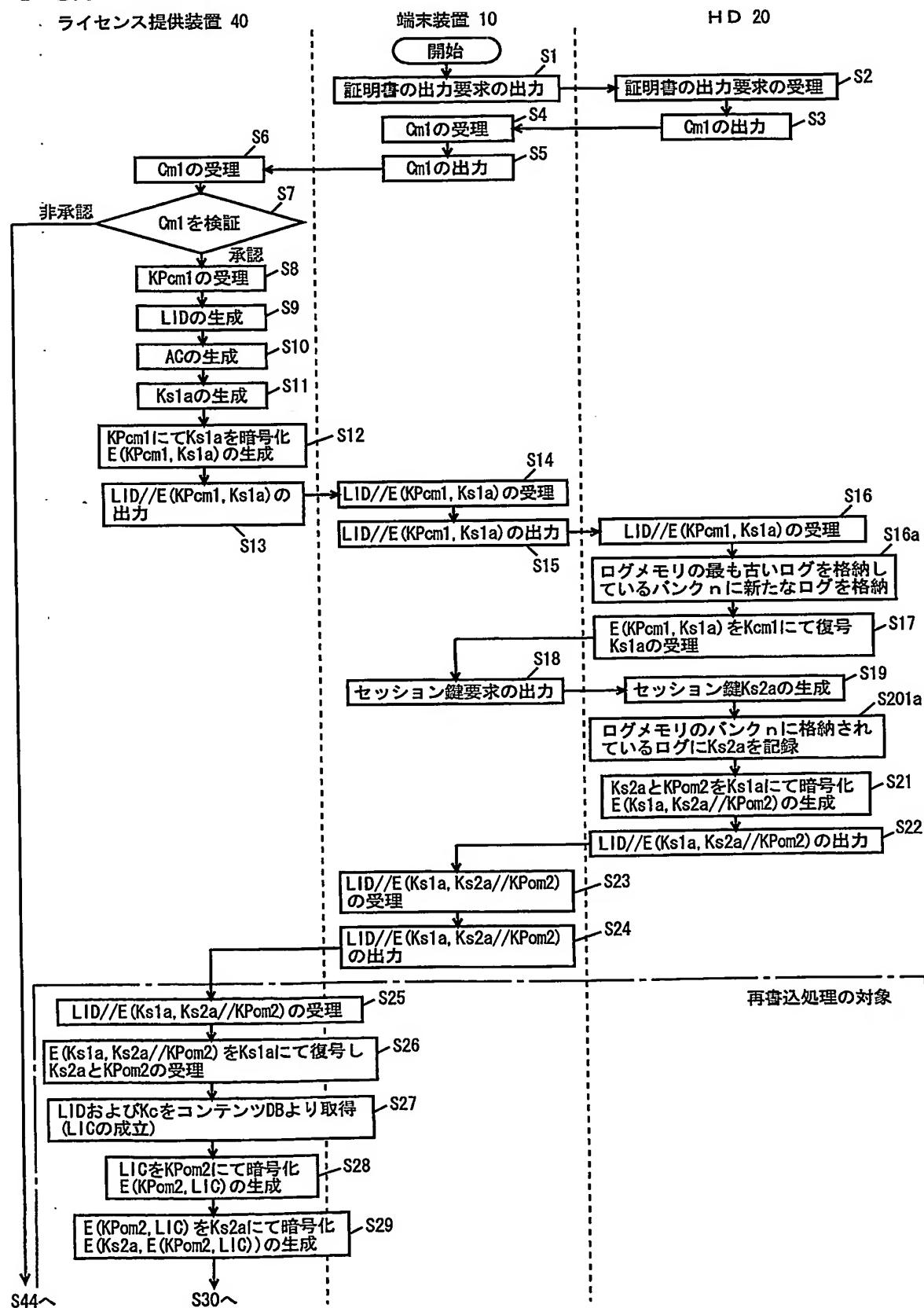


FIG. 26

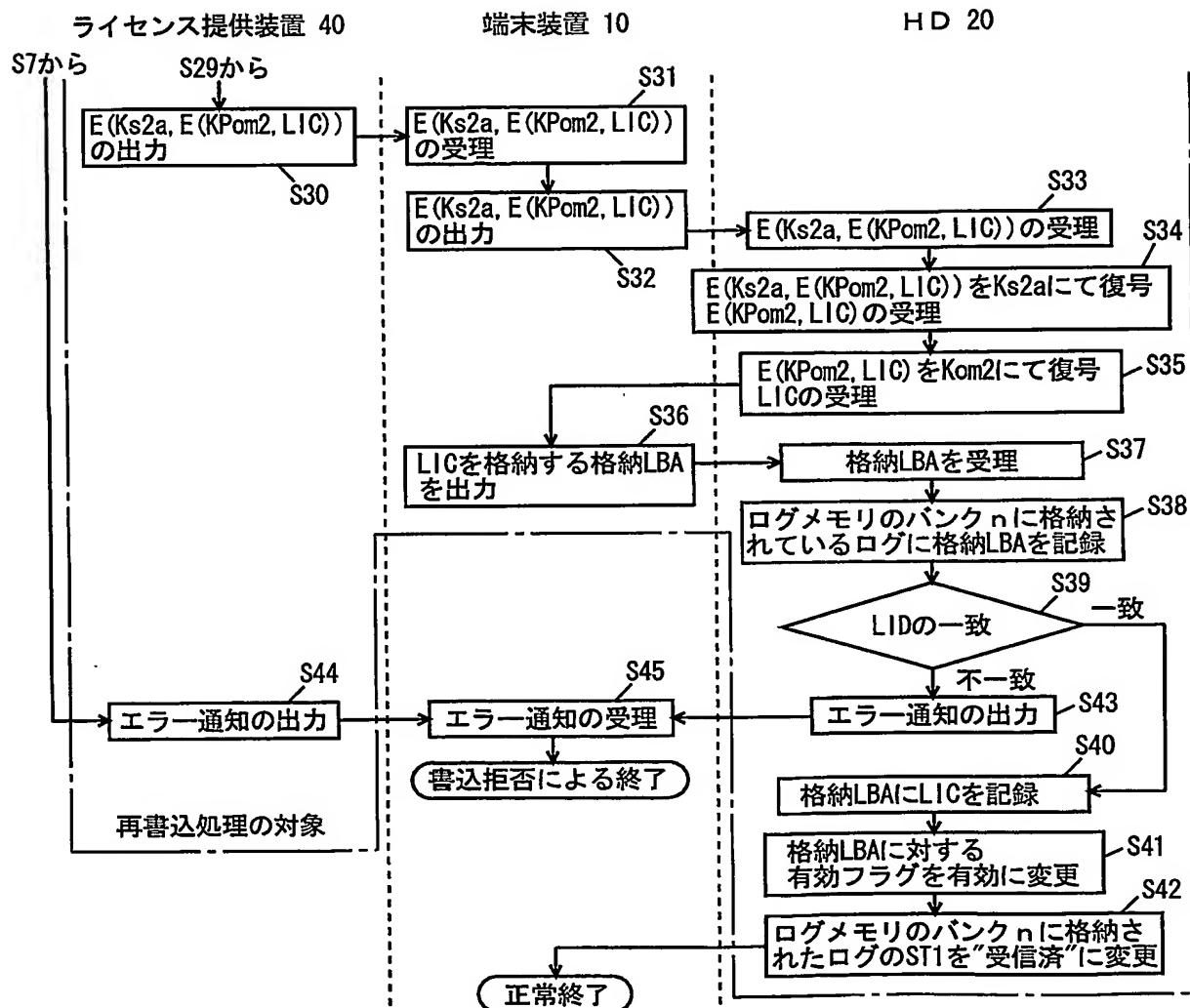


FIG. 27

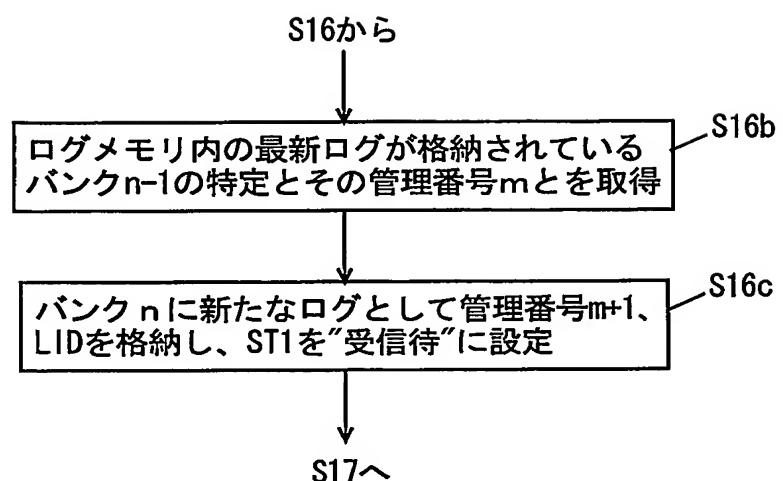


FIG. 28

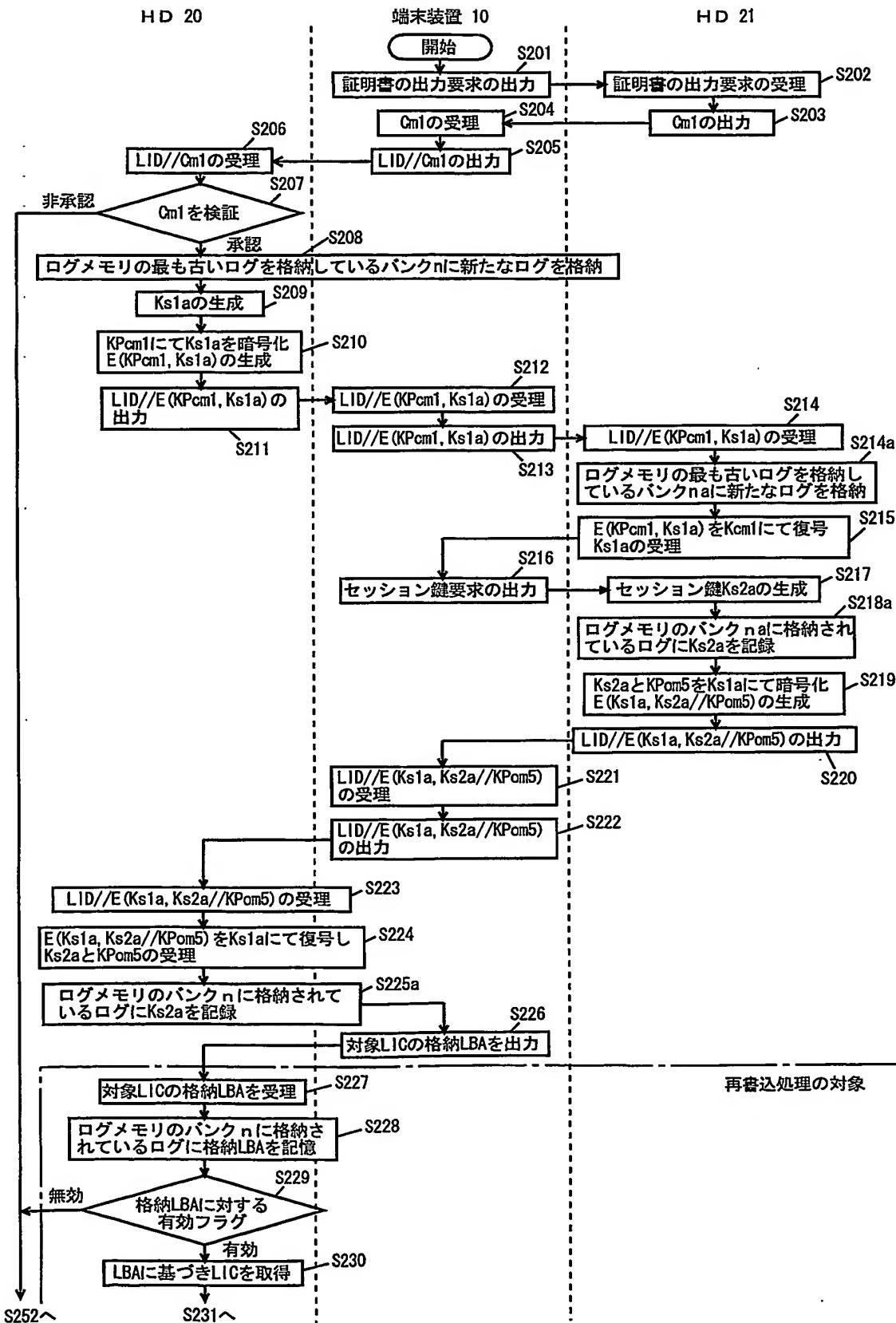


FIG. 29

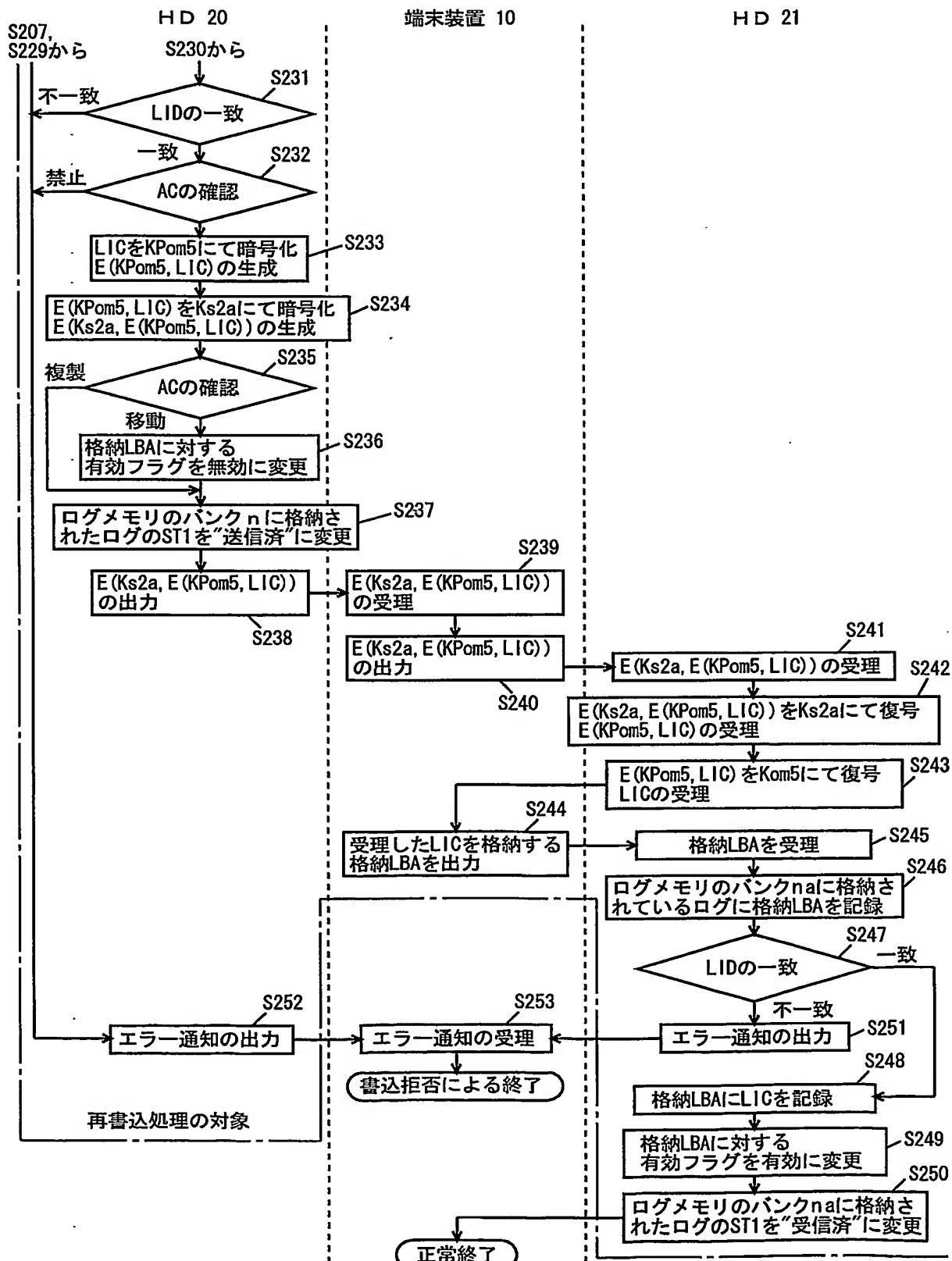
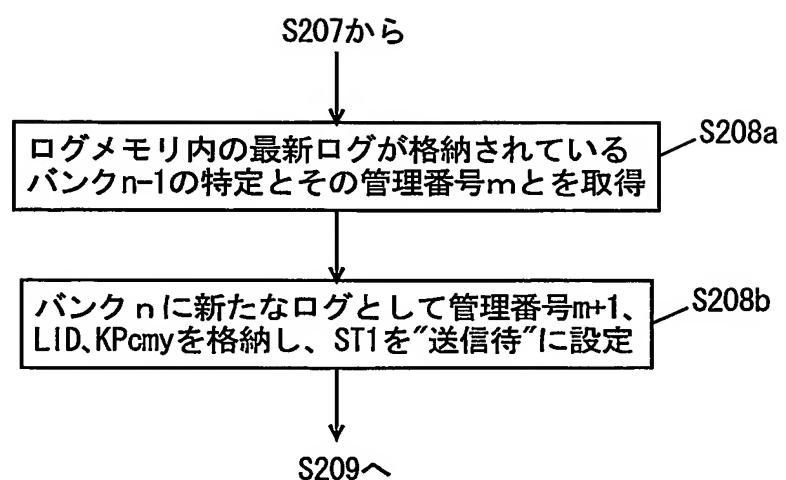


FIG. 30



**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP03/09414

**A. CLASSIFICATION OF SUBJECT MATTER**

Int.Cl<sup>7</sup> G06F12/14, G11B20/10, G06F3/06, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, G11B20/10, G06F3/06, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01/41356 A1 (Sanyo Electric Co., Ltd.), 07 June, 2001 (07.06.01), All drawings; all pages; in particular, description, page 5 & EP 1237324 A1	1-9
Y	JP 2002-189648 A (Hitachi, Ltd.), 05 July, 2002 (05.07.02), All pages; all drawings; in particular, Par. Nos. [0025] to [0029] (Family: none)	1-9
Y	JP 2001-197292 A (Konica Corp.), 19 July, 2001 (19.07.01), All pages; all drawings; in particular, Par. No. [0052] (Family: none)	1-9

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 15 October, 2003 (15.10.03)	Date of mailing of the international search report 28 October, 2003 (28.10.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP03/09414

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-39450 A (Mitsubishi Electric Corp.), 12 February, 1999 (12.02.99), All pages; all drawings; in particular, Par. Nos. [0002] to [0005] (Family: none)	1-9
Y	JP 6-202926 A (Fuji Xerox Co., Ltd.), 22 July, 1994 (22.07.94), All pages; all drawings; in particular, Par. No. [0005] (Family: none)	1-9
Y	JP 5-46359 A (Mitsubishi Electric Corp.), 26 February, 1993 (26.02.93), All pages; all drawings; in particular, Fig. 4 (Family: none)	7-9

A. 発明の属する分野の分類(国際特許分類 (IPC))  
Int. Cl. 7 G06F12/14, G11B20/10, G06F3/06, H04N5/91

## B. 調査を行った分野

調査を行った最小限資料(国際特許分類 (IPC))  
Int. Cl. 7 G06F12/14, G11B20/10, G06F3/06, H04N5/91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926 - 1996 年
日本国公開実用新案公報	1971 - 2003 年
日本国登録実用新案公報	1994 - 2003 年
日本国実用新案登録公報	1996 - 2003 年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO 01/41356 A1 (三洋電機株式会社) 2001.06.07, 全図、全頁、特に、明細書第5頁 & EP 1237324 A1	1-9
Y	JP 2002-189648 A (株式会社日立製作所) 2002.07.05, 全図、全頁、特に、【0025】-【0029】段落 (ファミリーなし)	1-9
Y	JP 2001-197292 A (コニカ株式会社) 2001.07.19, 全図、全頁、特に、【0052】段落 (ファミリーなし)	1-9

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)  
「O」口頭による開示、使用、展示等に言及する文献  
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」同一パテントファミリー文献

国際調査を完了した日

15.10.03

国際調査報告の発送日

28.10.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

奥村 元宏



5N 3044

電話番号 03-3581-1101 内線 3585

C (続き) 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
Y	JP 11-39450 A (三菱電機株式会社) 1999. 02. 12, 全頁, 全図, 特に【0002】-【0005】段落 (ファミリーなし)	1-9
Y	JP 6-202926 A (富士ゼロックス株式会社) 1994. 07. 22, 全頁, 全図, 特に【0005】段落 (ファミリーなし)	1-9
Y	JP 5-46359 A (三菱電機株式会社) 1993. 02. 26, 全頁, 全図, 特に図4 (ファミリーなし)	7-9